FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Gestão integrada de access points Wi-Fi autónomos

Isabel Duarte Fragoso

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Orientador: Professor João Neves

22 de Julho de 2016

Resumo

As redes sem fios são atualmente o modo de acesso prioritário à Internet. A sua enorme evolução ao longo do tempo, juntamente com o compromisso de manter a compatibilidade com os produtos mais antigos, tem trazido alguns constrangimentos ao nível da gestão de redes e da implementação de mecanismos de segurança.

Para ultrapassar estes limites têm vindo a ser desenvolvidos *softwares* proprietários e equipamentos como os controladores: entidades centralizadas que gerem uma rede composta por vários APs (*Access Points*). Por norma, os APs geridos por *softwares* proprietários ou controladores, têm em comum um determinado fabricante, ou conjunto de fabricantes, e apresentam certas características que os permitem ser geridos. A utilização de controladores tem, pelo menos, dois inconvenientes: não permite a compatibilidade numa rede constituída por APs autónomos e não favorece a interoperabilidade entre fabricantes.

O principal objetivo deste trabalho foi o desenvolvimento de uma interface *web*, *open source*, com vista à gestão integrada de APs Wi-Fi autónomos, permitindo a interoperabilidade entre os diferentes fabricantes. Para o desenvolvimento desta ferramenta recorreu-se ao protocolo de gestão SNMP (*Simple Network Management Protocol*).

Em primeiro lugar foi feito um levantamento do estado da arte e um estudo de mercado, para se perceber o tipo de ferramentas já existentes. Segue-se uma recolha de informação sobre as MIBs (*Management Information Base*) existentes e fundamentais para a gestão dos APs através do protocolo SNMP.

Posteriormente foi desenvolvida a arquitetura da solução final, contando com a pesquisa e seleção automática dos APs da rede, bem como o desenvolvimento de módulos de acesso e alteração das configurações dos equipamentos. Foi possível obter-se informações sobre os APs como os seus endereços MAC (*Media Access Control*) e IP (*Internet Protocol*), as interfaces, os SSIDs (*Service Set Identifiers*), as VLANs (*Virtual Local Area Network*) e as estações associadas a cada equipamento. A sincronização entre os processos de leitura e escrita, foi também implementada, sendo fundamental para prevenir conflitos.

Por fim, todos os dados recolhidos são disponibilizados numa interface *web*, onde é possível ao utilizador requerer pesquisas de rede ou alterar configurações de APs ou SSIDs.

Abstract

Wireless networks are, nowadays, the most common way used to access the Internet. Its huge evolution and the commitment to maintain compatibility with older equipments, has brought some constraints to manage and implement security in most networks.

To overcome this problems, some proprietary softwares have been released, as well as some equipments such as controllers: centralized entities that can manage a network composed by several APs (Access Points). Usually these APs are from a selected group of vendors and present some characteristics that allow them to be manageable. Using these controllers has, at least, two inconvenients: it doesn't allow compatibility in a network composed by autonomous access points and it doesn't support interoperability between APs from different vendors. To develop this project it was used SNMP (Simple Network Management Protocol).

Firstly, it was done some research to understand what kind of tools already exist to solve this problem and what were the fundamental MIBs (Management Information Base) to manage APs using SNMP protocol.

Then, the solution was designed and implemented. With this tool it is possible to do an automatic search and selection of the existent APs on a required network, as well as access to the APs information such as MAC (Media Access Control) and IP (Internet Protocol) addresses, interfaces, SSIDs (Service Set Identifiers), VLANs (Virtual Local Area Network) and their associated stations. Synchronization between writing and searching processes was implemented as well, being a fundamental part to prevent conflicts.

Lastly, all the collected data is available in a web interface, the user may require researches of networks or changing APs or SSIDs configurations.

Agradecimentos

Esta dissertação representa o fim de um período muito intenso da minha vida. Representa uma vitória pessoal, o alcançar de um objetivo há muito desejado.

Agradeço, desde já, ao meu orientador, o Professor João Neves, por ser um dos responsáveis pelo meu gosto especial pela área da gestão de infraestrutura de redes e por todos os conselhos e apoio prestado ao longo desta dissertação.

Não tenho palavras suficientes para agradecer aos meus Pais, Filomena Duarte e Luís Fragoso. Tudo o que sou, devo-o a eles. Por nunca terem duvidado de que eu seria capaz, por terem sempre feito tudo o que estava ao seu alcance em prol do meu bem-estar, da minha educação e do meu sucesso. Obrigada por todo o *paitrocínio* e por toda a confiança depositada. São os melhores do mundo!

Ao meu irmão Pedro, por ser o meu irmão preferido! Por ser um exemplo seguir e por me mostrar, dia após dia, que tudo na vida é possível, com dedicação e empenho.

Aos meus avós, pelos mimos, pela força e pela esperança que sempre depositaram em mim, bem como a toda a minha restante família.

Não podia deixar de agradecer também ao meu namorado Carlos Rodrigues. Por acreditar sempre em mim, pela paciência, pelos conselhos, por todos os lanches improvisados ao longo do desenvolvimento desta dissertação. Obrigada por me fazeres verdadeiramente feliz.

Um agradecimento especial à Sofia Inácio, pela amizade, pelos bons conselhos, pelos almoços e cafés e por nunca me deixar desanimar. Ao João Silva, ao Eduardo Almeida, ao João Dias, ao Paulo Vaz, ao Tiago Ferreira e ao Carlos Leocádio, por me ouvirem, pelas dicas importantes e por me ajudarem a clarificar ideias ao longo da elaboração deste projeto.

Fazer o curso na FEUP sem amigas seria uma tarefa bem mais complicada. Obrigada às minhas meninas: à Inês Cunha, à Angela Pinheiro, à Catarina Terra e à Beatriz Magalhães, por estarem sempre lá para restabelecerem a minha sanidade mental, por todas as *girl talks*, por todas as gargalhadas e por toda a amizade.

O meu muito obrigada aos amigos que estiveram sempre comigo ao longo destes anos, sempre prontos a ajudar, a dar um conselho ou uma palavra de apoio: Eduardo Fernandes, José Araújo, Manuel Oliveira, Luís Amorim e José Pedro Perdiz.

Ao Miguel Freitas, ao Francisco Oliveira, ao André Coelho, ao Ricardo Sousa e ao António Pintor, por serem sempre os melhores companheiros de trabalhos de grupo. É um prazer terminar este ciclo ao vosso lado!

Por fim, agradeço também aos amigos de sempre: à Mariana Duarte, à Emília Araújo, ao Telmo Borges, ao Miguel Santos, ao Bruno Costa, ao Fábio Vasconcelos, ao Nelson Oliveira, ao Pedro Maia e ao Pedro Nuno Vilhena pela amizade e pelo carinho.

Isabel Duarte Fragoso

"Leave this world a little better than you found it."

Robert Baden-Powell

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

AP	*Access Point*
ACK	*Acknowledgement*
BSS	*Basic Service Set*
BSSID	*Basic Service Set Identifier*
DHCP	textitDynamic Host Configuration Protocol
DS	*Distributed System*
DSSS	*Direct Sequence Spread Spectrum*
EGP	*Exterior Gateway Protocol*
ESS	*Extended Service Set*
FHSS	*Frequency-Hopping Spread Spectrum*
FT	*Fast BSS Transition*
IBSS	*Independent Basic Service Set*
ICMP	*Internet Control Message Protocol*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISM	*Industrial, Scientific and Medical*
LAN	*Local Area Network*
MAC	*Media Access Control*
MIB	*Management Information Base*
MIMO	*Multiple-Input Multiple-Output*
MTU	*Maximum Transmission Unit*
NMS	*Network Management Stations*
OFDM	*Orthogonal Frequency Division Multiplexing*
OSI	*Open System Interconnection*
OUI	*Organizational Unique Identifier*
PDU	*Protocol Data Units*
PHY	*Physical*
RADIUS	*Remote Authentication Dial In User Service*
RSNA	*Robust Security Network Association*
SAE	*Simultaneous Authentication of Equals*
SGMP	*Simple Gateway Monitoring Protocol*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSID	*Service Set Identifier*
STA	*Station*
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transfer Protocol*
UDP	*User Datagram Protocol*
UNII	*Unlicensed National Information Infrastructure*
VLAN	*Virtual Local Area Network*
WLAN	*Wireless Local Area Network*

Capítulo 1

Introdução

1.1 Tema

Hoje em dia é possível conectarmo-nos à Internet nos mais diversos locais: em casa, no trabalho, na escola, em aeroportos, hotéis ou até em restaurantes. Para isso, basta utilizar um dispositivo com capacidade para se ligar a uma rede Wi-Fi. O crescimento exponencial da utilização de *smartphones* incrementou a importância das redes Wi-Fi no quotidiano dos utilizadores comuns.

As redes Wi-Fi em estudo são redes sem fios baseadas na especificação IEEE 802.11 [1]. A criação da norma IEEE 802.11 e a sua notável evolução, a partir de 1999, possibilitaram a interoperabilidade e compatibilidade de produtos de diferentes fabricantes e características diversas, tornando-a o modo de acesso prioritário à rede local para conexão à Internet.

As redes sem fio baseadas na norma IEEE 802.11 são redes cada vez mais utilizadas, com diversas vantagens comparativamente às redes Ethernet, nomeadamente: a sua fácil instalação, a possibilidade de alcançarem lugares que as redes com fios por vezes não conseguem, e o facto de permitirem uma maior mobilidade dentro da área abrangida por uma determinada rede. As redes Wi-Fi também permitem a interoperabilidade, uma vez que o seu desenvolvimento se focou em manter o compromisso de compatibilidade com produtos desatualizados e a escalabilidade, sendo possível adicionar várias estações e/ou pontos de acesso a estas redes sem grandes alterações na sua estrutura inicial.

Atualmente é necessário lidar com os constrangimentos das redes Wi-Fi que se relacionam, principalmente, com a gestão e segurança. Uma das possibilidades para ultrapassar estes problemas é a utilização de interfaces de gestão comum, utilizando um protocolo de gestão de redes. O SNMP (*Simple Network Management Protocol*) é uma norma do IETF (*Internet Engineering Task Force*) daí ser um protocolo de gestão de redes muito utilizado para recolher informação e configurar equipamentos de rede que tem como vantagem a sua simplicidade.

O problema da gestão de redes estende-se também aos APs (*Access Points*) – entidades Wi-Fi, utilizados para transmitir e receber informação de e para estações, através de ondas rádio. Manter uma configuração consistente por todos os APs, numa determinada WLAN (*Wireless Local Area Network*), é uma tarefa complicada, mas extremamente relevante para prevenir a ocorrência de

erros ou conflitos. Um SSID (*Service Set IDentifier*) é o parâmetro que define o nome utilizado para identificar uma rede sem fios 802.11. A sua coerência é imprescindível: os APs pertencentes à mesma rede deverão ter SSIDs iguais.

A prevenção de interferências passa por fazer com que os canais definidos no AP não sofram sobreposição de outros canais adjacentes.

A natureza dinâmica e a partilha dos meios sem fios requer uma coordenação entre todos os APs, de modo a minimizar a interferência nesses meios e a maximizar a performance da rede.

Neste contexto, podem-se considerar três arquiteturas de redes sem fios (WLAN) [2]:

- **Autónoma** – cada AP é um simples equipamento que implementa todos os serviços 802.11, incluindo a parte da distribuição e integração de serviços. Estes APs são autónomos em todas as suas funcionalidades e não é necessário nenhum suporte de outros dispositivos. Neste tipo de arquiteturas os APs são configurados e controlados autonomamente e podem ser geridos através de protocolos de gestão de redes, tal como SNMP. Estes APs autónomos também são comummente denominados de *Fat APs* ou *Standalone APs*.

- **Centralizada** – na arquitetura centralizada são utilizados um ou mais controladores centralizados para a gestão de vários APs. O controlador tem como funções gerir, controlar e configurar os APs presentes na rede sob o seu domínio.

- **Distribuída** – Os nós desta rede são capazes de formar uma rede distribuída entre eles. Uma rede *mesh wireless* é um exemplo desta arquitetura, onde os nós da rede comunicam com os seus vizinhos para se organizarem. Os APs, neste caso, encarregam-se dos dados e do controlo, sendo que o plano da gestão está entregue ao *software* de controlo. O controlador, nesta arquitetura, será virtual e passivo.

Presentemente as arquiteturas mais utilizadas são as baseadas em controladores, devido à maior facilidade de gestão: é uma solução mais centralizada, sendo apenas necessário configurar o controlador. Estas arquiteturas atribuem maior ou menor responsabilidade ao controlador, consoante o tamanho da rede a implementar. Para além disso, os controladores, por norma, apenas gerem os APs de um determinado fabricante ou de um conjunto limitado de fabricantes e só gerem APs que estejam predispostos a serem geridos por controladores.

Os APs autónomos estão ainda muito presentes nas infraestruturas de redes atuais. Estes APs podem conter algum conhecimento sobre os APs vizinhos mas não permitem interação. Assim sendo, seria pertinente desenvolver uma ferramenta centralizada que permitisse a interoperabilidade de vários APs provenientes de diferentes fabricantes. Esta ferramenta deveria permitir fazer uma gestão da infraestrutura de rede de uma forma simples, sem ser necessário recorrer a um controlador.

1.2 Objetivos

Esta dissertação tem como objetivo o desenvolvimento de uma interface *web* para a gestão integrada de APs Wi-Fi autónomos.

A gestão de uma infraestrutura de comunicações Wi-Fi suportada por APs deverá ser feita de uma forma centralizada e baseada no protocolo de gestão SNMP. Com o desenvolvimento desta ferramenta, pretende-se aceder aos SSIDs, às VLANs (*Virtual LANs*), à localização das estações, à identificação das estações ligadas e aos canais utilizados na transmissão de informação.

Estes objetivos foram alcançados, havendo algumas limitações nas informações retiradas, correspondendo a erros na implementação das MIBs por parte de alguns fabricantes.

1.3 Estrutura da Dissertação

Este relatório está dividido em cinco capítulos. Neste primeiro capítulo é realizada a introdução do tema e motivação deste trabalho.

No Capítulo 2, é feita a caracterização do problema 2.1. Seguidamente é feita uma introdução às redes sem fios na Secção 2.2, fazendo referências às redes WLAN e à norma IEEE 802.11. O protocolo SNMP presente na Secção 2.3 é aqui descrito: desde o modelo de gestão de redes até à informação de gestão. Por fim, é analisado o mercado na Secção 2.4.

No Capítulo 3 são analisadas as MIBs (*Management Information Base*), sendo que na Secção 3.1 é feito um estudo das MIBs públicas e normalizadas como a MIB-II e a MIB IEEE802dot11. Na Secção 3.2 são abordadas as MIBs dos fabricantes Cisco, D-Link e Aruba.

No Capítulo 4 é exposta a implementação do projeto, contando com a arquitetura na Secção 4.1, o desenvolvimento na Secção 4.2 e na Secção 4.3 é feita a verificação da solução apresentada.

Por fim, no Capítulo 5 apresentam-se as conclusões do trabalho, bem como sugestões para trabalho futuro.

Capítulo 2

Tecnologias e Análise do Mercado

Neste capítulo apresenta-se uma introdução ao tema desta dissertação: gestão centralizada de redes sem fios. Na primeira secção é feita a caracterização do problema, seguindo-se uma breve referência às redes sem fios, à norma IEEE 802.11 e aos *Access Points*. Posteriormente, é apresentada uma secção sobre o protocolo SNMP que irá ser utilizado durante a realização do projeto. Por fim, na última secção, é feito um estudo do mercado onde é possível conhecer as soluções proprietárias de gestão de redes sem fios já existentes.

2.1 Caracterização do problema

Os APs autónomos são muito comuns nas infraestruturas de redes atuais. O facto de serem configurados manualmente, de não conhecerem a rede à sua volta e de não permitirem a interação com os APs vizinhos, provoca a necessidade de se utilizar uma ferramenta para operações de gestão e de monitorização.

A vantagem de uma ferramenta, como uma interface *web*, *open source*, centralizada e disponível, independentemente do sistema operativo em que é utilizada, consiste em poder visualizar ou alterar as configurações dos APs, independentemente dos fabricantes e sem a necessidade de recurso a um *software* proprietário ou a um controlador.

Para uma eficiente gestão dos APs contidos numa rede será necessário:

- Fazer a pesquisa automática de uma rede ou uma gama de endereços IP requerida pelo utilizador, selecionando apenas, de todos os equipamentos presentes na rede, os APs com o protocolo SNMP ativo;
- Identificar os detalhes dos APs existentes, como o nome, a localização, o contacto, os endereços IP (*Internet Protocol*) e MAC (*Media Access Control*), o canal utilizado, o fabricante, o modelo e a versão;
- Enumerar as interfaces de cada AP, a sua descrição, o seu tipo e estado;
- Para cada AP, determinar os SSIDs, a VLAN a que pertencem, se é necessária autenticação nessa rede e perceber se os SSIDs se encontram em modo *broadcast* ou não;

- Identificar as estações conectadas a cada AP percebendo qual o seu nome, endereços MAC e IP, qual o AP e respetivo SSID ao qual se encontram associadas e qual o tipo de equipamento em questão;
- Alterar as configurações de detalhes do AP como o nome, o contacto, a localização, o endereço IP ou o canal;
- Alterar as informações relativamente aos SSIDs: o nome da rede, a VLAN e a permissão para *broadcast*.

2.2 Redes sem fios

2.2.1 WLAN

As WLANs são redes de comunicação sem fios e flexíveis, utilizadas em sistemas em que a mobilidade do utilizador é um requisito. Funcionam como alternativa ou complemento às redes com fios LAN (*Local Area Network*).

São utilizadas as gamas de radiofrequência ou infravermelhos para transmitir e receber dados através do ar, minimizando a necessidade das comunicações por fios. Para existir conectividade, o utilizador necessitará apenas de um dispositivo que contenha instalado um cartão de interface dentro das gamas de frequência permitidas. O acesso a redes LAN, através das redes sem fios, pode ser feito através de um AP, que suporta vários utilizadores conectados simultaneamente.

Durante a instalação de uma rede sem fios é preciso considerar diversos fatores designadamente [3]:

- **Alocação de frequências**: para existir conectividade entre todos os dispositivos da rede, estes deverão comunicar dentro da mesma banda de frequências que deverá ser bem definida;
- **Interferências e fiabilidade**: numa rede com fios apenas são realizadas comunicações entre terminais conectados fisicamente à rede. Por sua vez, numa rede sem fios, existem interferências que podem ser causadas por várias fontes, como eletrodomésticos ou máquinas, que poderão estar contidas nos limites físicos da rede e operando dentro da mesma banda de frequências;
- **Segurança**: Como as redes sem fio não estão limitadas a ligações físicas autorizadas e não se encontram limitadas a uma determinada área, existe a possibilidade de ocorrência de ataques de criptoanálise. Poderão, também, ser inseridas interferências propositadamente para destabilizar o sistema. Várias medidas devem ser consideradas para garantir a segurança numa rede sem fios, como a encriptação de mensagens e a autenticação dos remetentes utilizando assinaturas digitais;
- **Consumo de energia**: este é um aspeto importante na implementação das redes sem fios, vdevido às limitações existentes na capacidade de armazenamento das baterias dos aparelhos móveis;

- **Mobilidade**: os limites de transmissão de dados e as regras de reencaminhamento da informação entre redes e de um AP para um terminal, deverão ser analisadas, visto que a possibilidade de mobilidade dos utilizadores é a grande vantagem das redes sem fios;
- ***Throughput***: para serem suportadas várias transmissões ao mesmo tempo, devem ser utilizadas técnicas de *spread spectrum*.

As redes WLAN podem ser implementadas seguindo uma topologia *peer-to-peer* (exemplo das redes *ad hoc*) em que os clientes comunicam diretamente entre si. As redes baseadas em APs são as mais utilizadas, demonstrando a possível interoperabilidade entre as redes LAN e as redes sem fio. Os APs são usados para permitir que um cliente sem fios possa comunicar com qualquer equipamento com ou sem fios dentro da mesma rede permitindo, desta forma, o acesso à rede de equipamentos móveis. As redes sem fios podem também ser utilizadas para interligarem duas redes LAN de diferentes edifícios.

As redes sem fio com a vantagem de permitirem mobilidade, fazem com que o acesso a informação em tempo-real seja facilitado, sendo este acesso independente da localização do utilizador dentro da rede. A facilidade na implementação física da rede e a escalabilidade que as redes sem fio permitem, fazem destas as redes predominantes atualmente.

2.2.2 IEEE 802.11

Em 1997 o IEEE (*Institute of Electrical and Electronics Engineers*) desenvolveu uma norma, o IEEE 802.11 [1], para uniformizar as redes sem fios, face ao sucesso e à adesão das redes WLAN.

Esta norma teve como objetivo providenciar interoperabilidade entre redes com e sem fios, bem como entre equipamentos de diferentes fabricantes. O IEEE 802.11 especifica mecanismos que compreendem a camada de acesso ao meio (MAC) e a camada física (PHY - *Physical*), de acordo com o modelo de referência OSI (*Open System Interconnection*) [3]. Assim, é possível definir protocolos de gestão e serviços de acesso ao meio, bem como regras para os equipamentos fixos, portáteis e em movimento dentro de uma determinada área.

À versão original da norma IEEE 802.11 foram adicionadas algumas funcionalidades. Nesta versão era definida a utilização da técnica de espalhamento de espetro por salto em frequência (FHSS - *Frequency-Hopping Spread Spectrum*) e a técnica de espalhamento de espectro por sequência direta (DSSS - *Direct Sequence Spread Spectrum*), utilizando a banda ISM (*Industrial, Scientific and Medical*). Os canais eram subdivididos na gama das frequências compreendida entre 2.4 e 2.4835 GHz, sendo que o débito variava entre 1 e 2 Mbit/s. Ao longo do tempo foram publicadas adendas ao *standard* 802.11 original tendo em conta a melhoria do desempenho das redes sem fios, sendo criados diferentes grupos de trabalho correspondentes aos *standards* 802.11a, 802.11b, 802.11ac, 802.11g, 802.11n, entre outros, como se pode verificar na tabela 2.1.

2.2.2.1 Arquitetura

O *standard* IEEE 802.11 tem uma arquitetura descentralizada, visto que as decisões dependem das estações móveis constituintes da rede. Este tipo de arquitetura elimina possíveis *bottlenecks*

Standard	Descrição
802.11b	Esta alteração à norma original foi criada em 1999. Utiliza a técnica de espalhamento de espetro por sequência direta (DSSS) e opera na gama de frequências entre os 2.4 e os 2.4835 GHz na banda ISM. Este grupo de trabalho melhorou os débitos da norma original, atingindo 1, 2, 5.5 e 11 Mbps, dentro desta gama de frequências.
802.11a	Tal como a norma 802.11b, também esta foi criada em 1999. As operações são realizadas na banda de frequências UNII (*Unlicensed National Information Infrastructure*) situada nos 5 GHz. A vantagem de serem feitas nesta gama de frequências consiste em evitarem possíveis fontes de interferência por equipamentos que operam na banda dos 2.4GHz, como os dispositivos que utilizam Bluetooth e os micro-ondas, sendo que atualmente, cada vez mais equipamentos utilizam a banda de frequências UNII. O 802.11a utiliza uma tecnologia de *spread spectrum*, o OFDM (*Orthogonal Frequency Division Multiplexing*) e poderá atingir débitos de 6, 9, 12, 18, 24, 36, 48 e 54 Mbps.
802.11g	Este *standard* foi desenvolvido no ano de 2003 e transmite na banda dos 2.4 a 2.4835 GHz na banda de frequências ISM, tal como o 802.11b, permitindo débitos de 6, 9, 12, 18, 24, 36, 48 e 54 Mbps, utilizando DSSS e OFDM. Esta alteração à norma 802.11 tem a vantagem de permitir compatibilidade com os equipamentos 802.11b, visto operarem na mesma banda de frequências.
802.11n	Este *standard*, criado em 2009, distingue-se pela utilização de antenas MIMO (*Multiple-Input Multiple-Output*), permitindo débitos que variam entre entre 72 Mbps e os 600 Mbps, dependendo do número de antenas utilizadas e a largura de banda do canal (20 ou 40 MHz). Esta norma foi certificada pela *Wi-Fi Alliance*, opera nas gamas de 2.4GHz na banda ISM e 5 GHz na banda UNII, permitindo compatibilidade com todas as alterações às normas existentes.
802.11ac	Este *standard* foi desenvolvido em 2013, com o objetivo de melhorar a norma 802.11n. Assim, é possível utilizar até 8 antenas MIMO e a largura de banda dos canais foi melhorada para os 80 MHz. É, também, certificada pela *Wi-Fi Alliance*.

Tabela 2.1: Normas IEEE 802.11 [1].

que as redes centralizadas poderão introduzir e tem a vantagem de os erros serem localizados e independentes: um erro numa estação da rede não terá de influenciar diretamente todos os componentes dentro da mesma área. A arquitetura é flexível e pode suportar vários tipos de redes.

Segundo esta norma existem dois modos de operação da rede [4]: a implementação como infraestrutura de rede e a implementação como rede ponto-a-ponto (*ad hoc*). No primeiro modo é utilizada a interoperabilidade entre as redes WLAN e as redes com fio. A transição entre os dois meios é feita através de um AP. As redes ponto-a-ponto existem entre clientes sem fios e, normalmente, são criadas espontaneamente, não suportando acesso a redes com fios.

A arquitetura IEEE 802.11 é composta pelos seguintes elementos [1] [4]:

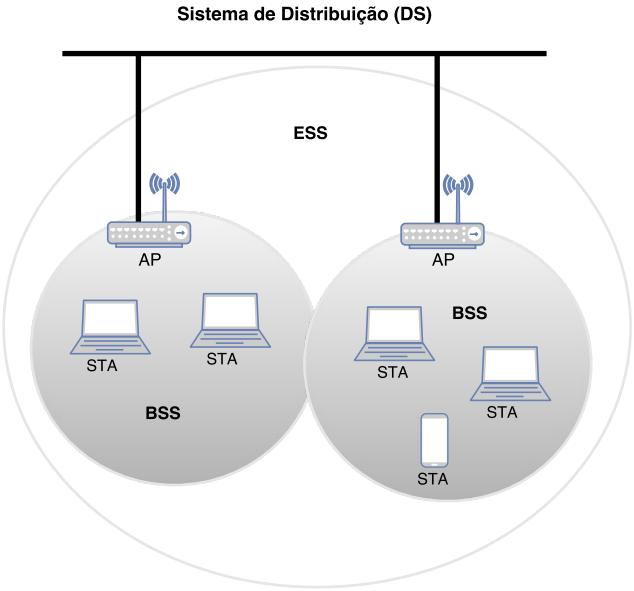


Figura 2.1: Modo de operação em infraestrutura, segundo a norma IEEE 802.11.

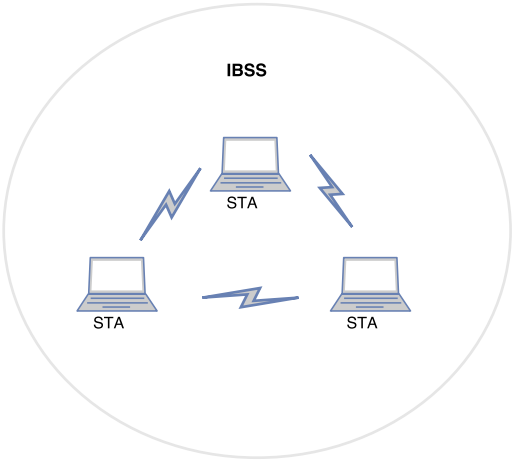


Figura 2.2: Modo de operação *Ad Hoc*, segundo a norma IEEE 802.11.

- **STA -** ***Station*** - Dispositivo que implementa as camadas física (PHY) e de acesso ao meio (MAC) da norma IEEE 802.11;
- **AP -** ***Access Point*** - Dispositivo que implementa todas as funcionalidades da estação (STA) e que providencia uma interface para as outras estações sem fios acederem ao sistema distribuído, ou seja, permite a operação da rede no modo de infraestrutura;
- **BSS -** ***Basic Service Set*** - Grupo de estações geridas por um AP;
- **DS -** ***Distributed System*** - Sistema que conecta vários BSS e que poderá integrar outras tecnologias de redes, como por exemplo a Ethernet;

- **ESS- *Extended Service Set*** - Grupo de um ou mais BSSs interligados através de um sistema de distribuição (DS), fazendo com que a área de cobertura seja maior. Para os dispositivos fora desta rede, o ESS oculta a mobilidade das estações, sendo que todas as suas estações móveis são vistas de fora como uma rede que contém uma camada MAC única.

- **IBSS - *Independent Basic Service Set*** - Sistema que utiliza o modo de operação *ad hoc*, não estando sobre o controlo de um AP. Uma rede IBSS inclui um número de nós ou estações sem fios que comunicam diretamente. Geralmente estas implementações têm uma área de cobertura limitada e não estão conectadas a nenhuma rede de grandes proporções, sendo criadas com um determinado objetivo bem definido;

2.2.3 Access Points

Os APs são elementos constituintes da arquitetura do *standard* IEEE 802.11 e providenciam uma interface que permite que as estações dentro da rede possam estabelecer comunicações sem fios. Normalmente o AP está ligado a uma rede com fios, permitindo que se estabeleça deste modo a operação entre redes com e sem fios.

Os APs podem ser inseridos em qualquer uma das três arquiteturas WLAN [2]: autónoma, centralizada ou distribuída, tal como já foi referido no Capítulo 1.

Na arquitetura centralizada, são utilizados controladores, com o objetivo de facilitar as operações de gestão e monitorização, sendo função do controlador gerir, controlar e configurar os APs presentes na rede sob o seu domínio. Já na arquitetura distribuída, os APs encarregam-se de comunicar com os vários nós para formarem uma rede distribuída entre eles, sendo o plano da gestão entregue ao *software* de controlo [2].

A primeira geração de APs surgiu depois da implementação da norma IEEE 802.11b em 1999. Estes, também conhecidos por APs autónomos, permitem a configuração dos seus parâmetros através do protocolo SNMP e não necessitam de suporte por parte de outros dispositivos. Incluem controlo de acesso baseado em listas ou filtros e contêm características específicas de suporte à segurança como autenticação e encriptação. Também o nível da potência transmitida e o canal escolhido podem ser manualmente configurados nestes dispositivos.

Para além das funcionalidades básicas oferecidas por um AP, estes também podem ser utilizados como repetidores ou *bridges* sem fios, funcionando como uma estação de *relay*, de modo a expandir a cobertura de um determinado AP ou fazendo a ligação entre duas redes.

A configuração dos AP depende, em grande parte, dos requisitos específicos do *hardware*, havendo assim diferentes parâmetros que podem ser configurados de acordo com as especificações de cada fabricante. No entanto, existem alguns parâmetros em comum [5]:

- **Endereço IP**: É neste campo que se irá atribuir a um AP um endereço IP, a máscara da *subnet* e a respetiva *default gateway*;

- **SSID**: Este é o parâmetro utilizado para identificar a rede. Para coexistirem diferentes redes sem fio no mesmo espaço é necessário que estas contenham diferentes SSID;

- **SSID *broadcast***: Caso esteja ativado, os APs divulgam os seus SSIDs na rede, para que os equipamentos dentro da sua área cobertura identifiquem a rede e se consigam conectar ao AP. Se esta funcionalidade estiver desativada, o cliente sem fios deverá conhecer previamente o SSID da rede onde se quer conectar;
- **Máxima potência transmitida**: Aqui é feita a seleção da máxima potência de transmissão permitida;
- **Canal**: Este parâmetro permite escolher o canal onde irão ser estabelecidas as comunicações. Para que não existam sobreposições entre os diferentes sinais de redes sem fios, deverão ser atribuídos os canais 1, 6 ou 11 ao AP;
- **Segurança**: Deverá ser feita a seleção dos modos de segurança, a escolha de uma *password* e do modo de autenticação;
- **Configuração da antena**: Poderá, também, ser feita a seleção de antenas específicas, sendo utilizada a que oferecer o melhor sinal;
- **Modo de operação**: É este parâmetro que indica se o AP está a ser utilizado como AP *bridge* ou *repeater*.

2.2.3.1 Canais

Nas redes sem fios cada estação precisa de se associar a um AP antes de enviar ou receber dados. Quando um administrador de rede instala um AP necessita de lhe atribuir um SSID, ou seja, um nome único aliado a uma determinada rede. O administrador terá também que atribuir ao AP um canal, dentro de uma lista de canais disponíveis [6].

Neste momento a norma IEEE 802.11 opera em cinco gamas de frequências diferentes: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz e 5.9 GHz. Cada banda é dividida em vários canais. Utilizando, como exemplo, o caso da banda operada na frequência dos 2.4 GHz aos 2.485 GHz: dentro destes 85 MHz é possível definir 14 canais parcialmente sobrepostos, utilizando uma largura de 22 MHz por canal. A largura requerida por cada canal depende do protocolo e do débito selecionado, bem como do ambiente eletromagnético onde os equipamentos se inserem [6]. Assim, neste caso concreto, só é possível obter canais que não se sobreponham se estes estiverem separados por 4 ou mais canais. Os canais 1, 6 e 11 são, assim, os únicos canais que cumprem este requisito e que podem ser utilizados para associar a cada AP. Se, neste caso, existirem três redes na mesma localização estas podem coexistir associando-se cada um dos três canais disponíveis por cada rede.

2.3 Protocolo SNMP

No mundo complexo e desafiante das tecnologias de rede, existem variadíssimos paradigmas, atribuindo-se assim, uma grande importância e relevo à normalização. É dentro deste ambiente, onde se encontram dispositivos como *routers*, *switches* e servidores, que a gestão de equipamentos

e serviços de redes passou a tomar um papel determinante no bom funcionamento e na melhoria do desempenho destes sistemas.

2.3.1 Modelo de gestão de redes SNMP

O SNMP é um conjunto de especificações desenvolvidas pelo IETF, com o objetivo de gerir redes IP, utilizando um protocolo simples. A versão original do SNMP derivou do protocolo SGMP (*Simple Gateway Monitoring Protocol*), em 1998, possibilitando a gestão de sistemas Unix e Windows, impressoras, entre outros equipamentos, desde que estes aceitem a aquisição de informação através de SNMP.

O modelo de gestão de redes SNMP é composto por quatro entidades fundamentais [7] [8] :

- **Estação de Gestão**: Posto de monitorização e controlo, onde o modelo de funcionamento é criado. Faz a ligação entre o gestor da rede e o sistema a gerir. O gestor da rede dispõe de um *software* que lhe permite lidar com as tarefas necessárias para a gestão da rede. Por vezes os gestores são denominados NMS (*Network Management Stations*), responsáveis por fazer *polling* e receber *traps* dos agentes da rede. A ação de *polling* consiste no envio de pedidos aos agentes para solicitar determinadas informações, enquanto que os *traps* são enviados pelos agentes para notificar a estação de gestão de eventos importantes;

- **Agente**: *Software* presente nos dispositivos que estão a ser geridos. Pode ser um programa separado ou poderá estar incorporado no sistema operativo. Hoje em dia, a maioria dos equipamentos IP já vêm com um agente SNMP incluído. Os agentes providenciam informação de gestão para a estação de gestão. São responsáveis por responder aos pedidos enviados e de enviar autonomamente informação importante para a estação de gestão. Eventualmente poderão receber da estação de gestão pedidos para a alteração dos seus valores;

- **Protocolo de Gestão**: O protocolo de gestão é utilizado na comunicação entre a estação de gestão e os agentes, especificando os seguintes tipos de operação:

  - ***get*** - permite à estação de gestão consultar um determinado parâmetro de um agente;
  - ***set*** - permite à estação de gestão modificar um determinado parâmetro de um agente;
  - ***trap*** - permite que cada agente notifique a ocorrência de eventos extraordinários à estação de gestão.

- **Informação de Gestão**: O SNMP por si só não define a informação que um sistema a ser gerido oferece. Esta é definida pelas MIBs (*Management Information Base*). As MIBs podem conter um conjunto de objetos, ou seja, um conjunto de variáveis que caracterizam um determinado equipamento, tais como o tempo de operação, contacto, nome, localização, entre outros. A função das MIBs é guardar as informações dos agentes de uma forma acessível à estação de gestão. Os objetos são normalizados para determinadas categorias de equipamentos;

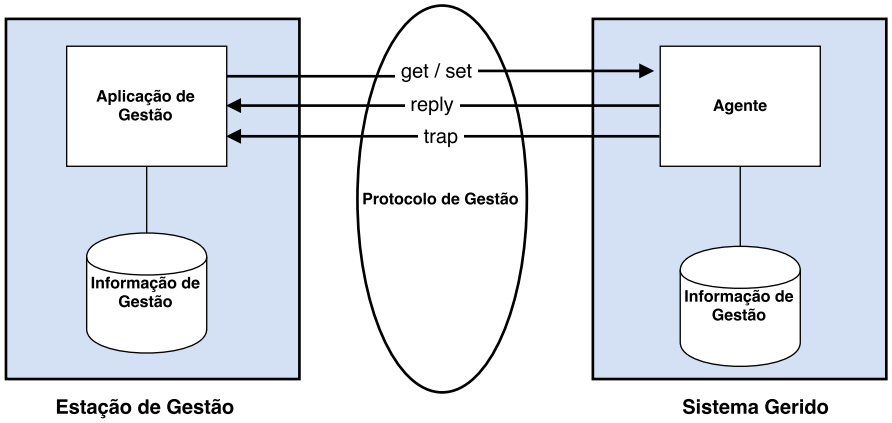


Figura 2.3: Arquitetura do protocolo SNMP [7].

2.3.1.1 Protocolo de Gestão

O SNMP utiliza UDP (*User Datagram Protocol*) como o protocolo de transporte para transmitir mensagens entre o agente e a estação de gestão. O UDP foi escolhido em detrimento do TCP (*Transmission Control Protocol*), visto não depender de uma conexão ponto-a-ponto feita entre o Agente e o NMS e devido ao menor *overhead* introduzido. Este protocolo de transporte apenas é critico no caso dos *traps*, visto que os agentes enviam a notificação, mas caso esta nunca chegue à estação de gestão, o NMS não irá ter maneira de saber que esse *trap* alguma vez foi enviado e o agente não saberá que tem de o reenviar. O SNMP poderá, também, utilizar o TCP como protocolo de transporte, não sendo aconselhado, devido ao congestionamento da rede com *acknowledgements* [8].

Assim sendo, o SNMP utiliza UDP na porta 161 para enviar e receber pedidos e utiliza a porta 162 para receber *traps* dos agentes [8].

O PDU (*Protocol Data Units*) é uma unidade de informação transmitida entre dois nós. Esta trama contém informações sobre a versão do protocolo, a *community string* e a mensagem a enviar, contendo o tipo de PDU, o ID do pedido e os valores dos objetos [8].

A *community string* é utilizada no serviço de autenticação limitando o acesso: é apenas concedido a estações autorizadas, de forma a permitir diferentes privilégios consoante as diferentes estações de gestão. A *community string* é, também, utilizada de modo a que uma estação gerida possa funcionar como *proxy* para outras estações.

No processo de autenticação, as *community strings* são únicas e funcionam como *passwords*. As estações de gestão pertencentes a uma comunidade apenas necessitam de indicar a *community string* para aceder ao agente em questão [9].

SNMPv1

A primeira versão da arquitetura SNMP é simples, centralizada e rígida. São especificados cinco PDUs [10]:

- **GetRequest**: Pedido enviado por parte do gestor para o agente com o objetivo de aceder ao valor de uma das variáveis. O tipo de PDU na trama fica preenchido com o valor 0;

- **GetNextRequest**: Pedido do gestor para o agente, de forma a descobrir as variáveis disponíveis para gestão e quais os seus valores. O tipo de PDU na trama fica preenchido com o valor 1;

- **GetResponse**: Resposta do agente às operações *GetRequest*, onde retorna o valor da variável em questão, e *GetNextRequest* contendo a resposta com a variável seguinte da estrutura de dados, ou para confirmar a operação *SetRequest*. O tipo de PDU na trama fica preenchido com o valor 2;

- **SetRequest**: Pedido do gestor para que o agente altere o valor de uma determinada variável. O tipo de PDU na trama fica preenchido com o valor 3;

- **Trap**: Notificação proveniente do agente e enviada para o gestor, indicando um evento significativo. Esta mensagem é enviada automaticamente para o gestor. O tipo de PDU na trama fica preenchido com o valor 4.

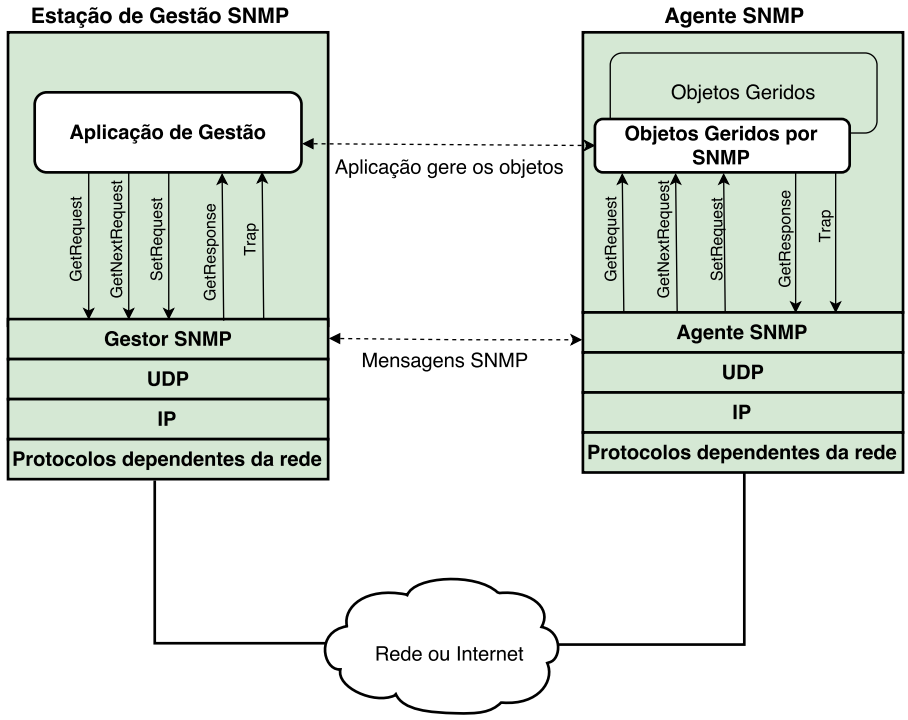


Figura 2.4: Modelo de gestão de redes SNMPv1 [11].

Os mecanismos de segurança associados a esta versão do protocolo SNMP existem mas são limitados, visto que a *community string* é enviada em claro entre o agente e a estação de gestão.

SNMPv2

Com o aumento do número de utilizadores, foi sentida a necessidade de acrescentar mais funcionalidades, particularmente no que diz respeito à questão da segurança. O SNMPv1 apresentava limitações na gestão de grandes redes, devido ao *polling*, capaz de criar problemas de desempenho. A versão anterior também não era adequada para a transferência de grandes quantidades de informação e as mensagens *trap* não eram confirmadas, pelo que não havia garantia de que mensagens criticas fossem entregues.

Nesta nova versão do SNMP, o desempenho melhorou e houve alteração dos formatos das PDUs já existentes. Para além disso, foi implementado o suporte em múltiplos protocolos e introduzidas quatro novas PDUs [12]:

- **GetBulkRequest**: Versão otimizada do *GetNextRequest* - permite pedir várias instruções desta operação melhorando a eficiência da operação de percorrer e descobrir as diferentes variáveis num agente. O tipo de PDU na trama fica preenchido com o valor 5;
- **InformRequest**: Utilizada na comunicação entre estações de gestão. O tipo de PDU na trama fica preenchido com o valor 6;
- **SNMPv2-Trap**: Substitui o *Trap* do SNMPv1. Difere essencialmente no formato da PDU. O tipo de PDU na trama fica preenchido com o valor 7;

A operação *Trap* da primeira versão do protocolo foi substituída pela operação *SNMPv2-Trap*, mas as restantes operações do SNMPv1 continuam a ser suportadas.

Nesta segunda versão do protocolo foi feita uma tentativa de implementação de novos mecanismos de segurança no SNMP, no entanto não foram estabelecidas medidas consensuais e robustas, tornando este protocolo mais complexo e inadequado para algumas operações de configuração.

SNMPv3

No SNMPv3 mantém-se o modelo de gestão de redes do protocolo SNMPv1: um ou mais nós para serem geridos, cada um contendo uma entidade SNMP que permite aceder à informação de gestão do nó e, pelo menos, uma entidade SNMP de gestão com uma ou mais aplicações de gestão da rede instaladas. Assim, as noções agente e estação de gestão deixaram de ser utilizadas, dando lugar às entidades SNMP. Cada entidade é composta por um SNMP *Engine*, responsável por enviar, receber, autenticar e encriptar mensagens, bem como controlar o acesso aos objetos geridos, e por uma ou mais SNMP *Applications* que utilizam os serviços fornecidos pelo motor SNMP para realizarem as suas operações [9].

No SNMPv3 foram criadas alterações utilizando algumas áreas omissas na versão 2, melhorando a capacidade de configuração remota e assegurando a confidencialidade, ou seja, aplicando encriptação aos pacotes enviados. A integridade é também tida em conta, garantindo que os pacotes não são alterados ou a sua ordem modificada. Por sua vez, a autenticação é feita para que seja possível verificar que as mensagens foram enviadas a partir fontes válidas. Outra caraterística do SNMPv3 é a sua modularidade.

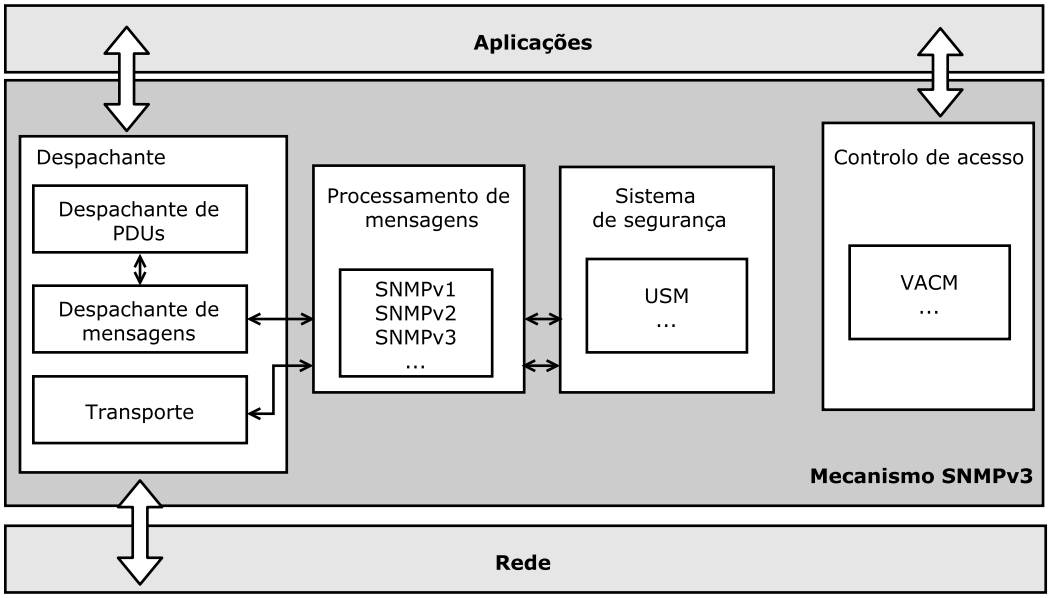


Figura 2.5: Arquitetura do SNMPv3 [9].

Quando uma mensagem é emitida, o *dispatcher* verifica a versão e o tipo de protocolo selecionado, invocando o processador de mensagens adequado (SNMPv1, v2 ou v3). A mensagem é em seguida entregue ao módulo de segurança para depois ser enviada. Quando uma mensagem é recebida, é analisada pelo *dispatcher* e em seguida é enviada para o processamento de mensagens. Finalmente, é incluída numa etapa de autenticação, descodificação e deteção de atrasos.

O principal objetivo do SNMPv3 é resolver a questão da segurança, sendo atualmente suportado por vários fabricantes.

2.3.2 Informação de gestão

Uma MIB é a coleção estruturada de objetos, ou seja, de dados a serem geridos, como o tempo de operação, o contacto, o nome e o número de interfaces de um dispositivo. A MIB no protocolo SNMP surge como uma base de dados organizada em árvore, que contém informações sobre o estado dos recursos geridos pelos sistema [9].

Para que as MIBs sejam utilizadas de uma maneira eficaz pelos sistemas de gestão, os objetos que caracterizam um recurso específico devem ser os mesmos para cada sistema e deve ser definida uma estrutura comum de representação e gestão da informação. A SMI (*Structure of Management Information*) descreve o formato da definição do objeto gerido: providencia uma maneira de definir os objetos especificando, desta forma, o modo como são definidas e construídas as MIBs.

As MIBs podem ser públicas ou privadas. As MIBs privadas contêm informações específicas dos equipamentos, tais como configurações e colisões, de uma determinada organização.

Os objetos geridos contêm três atributos: o nome, o tipo e sintaxe e a codificação [7][8].

- **Nome dos Objetos**: Identifica univocamente o objeto, sendo também denominado como OID (*Object Identifier*). É representado por uma sequência de números inteiros ou nomes separados por pontos. A cada nome coincide um número único. Cada OID identifica uma variável que pode ser lida ou alterada através do SNMP.

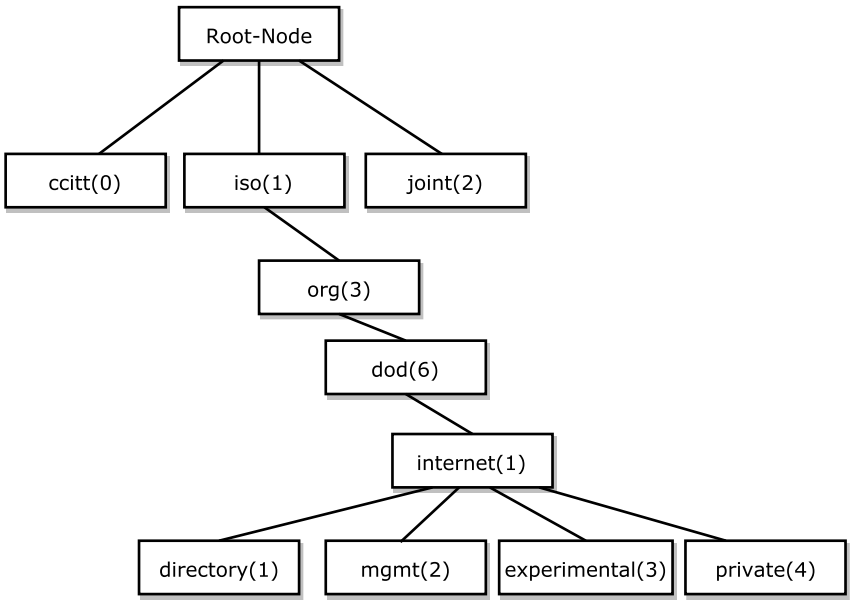


Figura 2.6: MIBs: Árvore dos objetos [8].

A partir da raiz da árvore dos objetos, representada na Figura 2.6, pode-se observar que são definidos três ramos: o *ccitt(0)*, referente aos objetos geridos pelo CCITT (*Comité Consultatif International Téléphonique et Télégraphique*), agora ITU (*International Telecommunication Union*), o *iso(1)*, referente aos objetos geridos pela ISO (*International Organization for Standardization*) e o *joint(2)*, referente aos objetos geridos em conjunto pelas duas entidades.

O ramo *iso(1)* é o único que contém uma *subtree* a *iso(1).org(3).dod(6).internet(1)*. Assim sendo, o ramo *internet(1)* terá um OID único: 1.3.6.1, que pode também ser representado por *iso.org.dod.internet*.

Abaixo do nó *internet(1)* são definidos quatro ramos, tal como se pode verificar na Figura 2.6 [13]:

- ***directory(1)***: reservado para utilização com o diretório OSI (X.500);
- ***mgmt(2)***: também denominado como *management*, é utilizado para definir um conjunto de standards de gestão dos objetos da Internet;
- ***experimental(3)***: usado para identificar objetos utilizados em experiências e em investigações;

- ***private(4)***: utilizado para identificar objetos definidos unilateralmente, ou seja, é utilizando este ramo que é feita a definição dos objetos próprios de cada organização, sendo que estas ficam responsáveis pela sua gestão.

- **Tipo e Sintaxe** [8]: O tipo do objeto é definido utilizando o ASN.1 (*Abstract Syntax Notation One*). Esta linguagem é utilizada para especificar como é que a informação transmitida é representada entre a estação de gestão e o agente. Ou seja, serve apenas para definir o tipo de informação que o objeto gerido pode suportar.

  Os tipos de dados suportados pelo SMIv1 são: *INTEGER*, *OCTET STRING*, *OBJECT IDENTIFIER*, *NULL*. Descrevem, assim, a maneira como podem ser representados os objetos geridos, permitindo inteiros, *strings* e os OIDs, no formato já referido anteriormente. O *Counter* é utilizado para fazer um acompanhamento da informação, como por exemplo saber o número de octetos enviados ou recebidos. Este número é sempre incrementado e quando o valor máximo é atingido, o contador retorna ao valor zero. Ao contrário do contador, o *Gauge* pode ser incrementado ou decrementado, desde que o seu número máximo nunca seja atingido. O *SEQUENCE* e o *SEQUENCE OF* permitem a construção de listas e tabelas. O *IpAddress* e o *NetworkAddress* representam endereços, sendo que este último poderá representar diferentes tipos de endereços de rede. O *TimeTicks* é utilizado para representar o tempo em centésimos de segundo e o *Opaque* permite armazenar qualquer outro tipo ASN.1 numa *OCTET STRING*.

  A linguagem ASN.1 possibilita a criação de Macros, permitindo a extensão da linguagem. Assim, com o aparecimento da segunda versão do protocolo SNMP, foi criada também uma segunda versão da SMI, mantendo e expandindo a estrutura original: a SMIv2. Nesta segunda versão é possível ter um maior controlo sobre a maneira como se acede ao objeto. Tal como se pode verificar na árvore dos objetos representada na Figura 2.7, foi acrescentado um ramo para esta segunda versão da SMI, contendo o ramo snmpV2 com OID 1.3.6.1.6.

- **Codificação**: Cada instância de um objeto gerido é codificada utilizando o BER (*Basic Encoding Rules*).

2.4 Estudo do mercado

Tal como referido no Capítulo 1, o objetivo deste projeto incide sobre a arquitetura WLAN autónoma. Esta arquitetura contém APs autónomos que podem conter conhecimento sobre os APs vizinhos, mas não permitem interação.

A maioria dos equipamentos fornece *software* de gestão e monitorização próprio, apresentando o inconveniente de ser específico para um determinado tipo de equipamento, e contendo, por vezes, permissões de gestão dos APs muito reduzidas. A gestão dos controladores e dos APs autónomos existentes dentro de uma determinada área, é feita através destas interfaces. Estes APs para poderem ser geridos necessitam de pertencer à gama de fabricantes autorizados pela ferramenta e precisam de apresentar características próprias para poderem ser geridos.

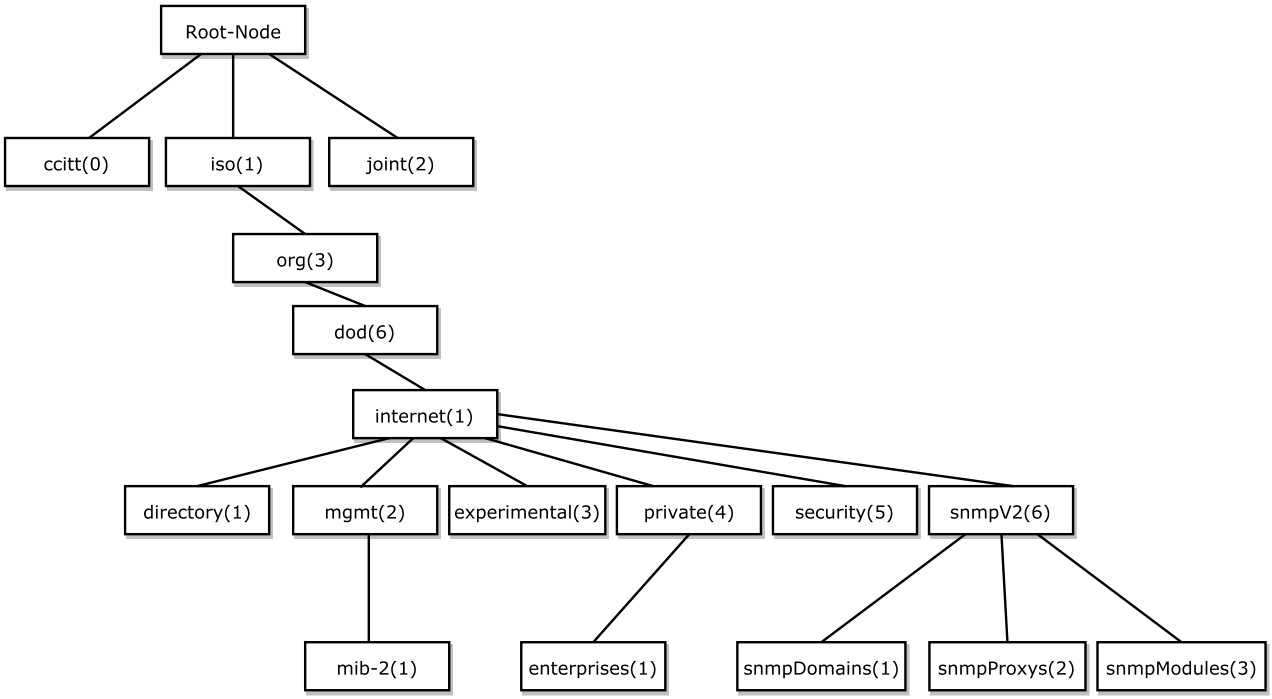


Figura 2.7: Árvore dos objetos para a nova versão: SMIv2 [14].

Alguns fabricantes de *hardware* fornecem soluções de monitorização, bem como os próprios APs, estando estes por vezes disponíveis para funcionarem como autónomos ou sob o domínio de um controlador. As informações sobre fabricantes, *software* utilizado e os respetivos APs, estão disponíveis na tabela 2.2. Para a elaboração desta tabela foi tido como critério de seleção o facto de o fabricante revender em Portugal, daí não serem incluídos determinados *softwares*, nomeadamente pertencentes à Xirrus e Huawei.

Após analisar os cinco *softwares* apresentados na tabela 2.2, foi verificada alguma dificuldade na monitorização conjunta de APs de diferentes fabricantes:

- ***HP IMC Wireless Services Manager Software*** [15] - permite a monitorização de alguns modelos de APs de três fabricantes diferentes: HP, Cisco e Aruba e monitoriza o desempenho dos APs autónomos e controlados.

- ***Cisco Prime Infrastructure*** [16] - *software* muito completo, contendo variadíssimas funcionalidades, desde a monitorização de APs até ao apoio a redes WAN. Permite a monitorização de APs apenas pertencentes à Cisco.

- ***AirWave*** [17] - pode ser utilizado em qualquer rede e descobre automaticamente os equipamentos de uma rede WLAN. Suporta APs de vários fabricantes como Cisco, Motorola e HP, mas as funcionalidades poderão variar entre equipamentos.

Proprietário	Software	APs
Hewlett Packard	HP IMC Wireless Services Manager Software [15]	- HP M220-802.11n AP series - HP MSM-802.11n Dual Radio AP series - HP MSM-802.11n Dual Radio indoor/outdoor AP series
Cisco Systems	Cisco Prime Infrastructure [16]	- Cisco Aironet 802.11n G2 series indoor AP 600, 700W, 1600, 2600, 3600 series - Cisco Aironet 802.11ac G2 series indoor AP 1700, 2700, 3700 series
Aruba	AirWave [17]	- Aruba 320 series 802.11ac wave2 - Aruba 220 series 802.11ac - Aruba 228 - Aruba 210 series 802.11ac - Aruba 200 series 802.11ac - Aruba 110 series 802.11n - Aruba 103 series 802.11n
Ruckus	Ruckus Unleashed [18]	- R500 - R600
Ubiquiti	UniFi Controller Software [19]	- UniFi AP - UniFi AP - LR - UniFi AP - PRO - UAP - AC

Tabela 2.2: Soluções de monitorização proprietárias

- ***Ruckus Unleashed*** [18] - este *software* é personalizado para redes que contêm até 25 APs, sem qualquer tipo de controlador. É compatível apenas com os APs da Ruckus R500 e R600.

- ***UniFi Controller Software*** [19] - apesar dos APs da UniFi serem independentes de um controlador, não funcionam sem a instalação deste *software*, não existindo qualquer tipo de interoperabilidade com outros equipamentos de diferentes fabricantes.

Dentro destas cinco opções, o *software AirWave* é o que possibilita uma maior flexibilidade,

possibilitando a monitorização de APs pertencentes a um maior leque de fabricantes: Aruba, Brocade, Alcatel-Lucent, Dell, Juniper, Cisco, Arista e HP.

O *User Device Tracker* [20] da SolarWinds, é uma ferramenta proprietária, que permite a monitorização de vários dispositivos de rede, o mapeamento das portas dos comutadores e a procura de equipamentos através do seu endereço MAC ou IP, nas redes com e sem fios. Este *software* suporta todos os fabricantes, permitindo criar uma lista de permissão de dispositivos para diferenciar os equipamentos "seguros"dos restantes. Este *software* está limitado ao sistema operativo Windows e utiliza SNMP.

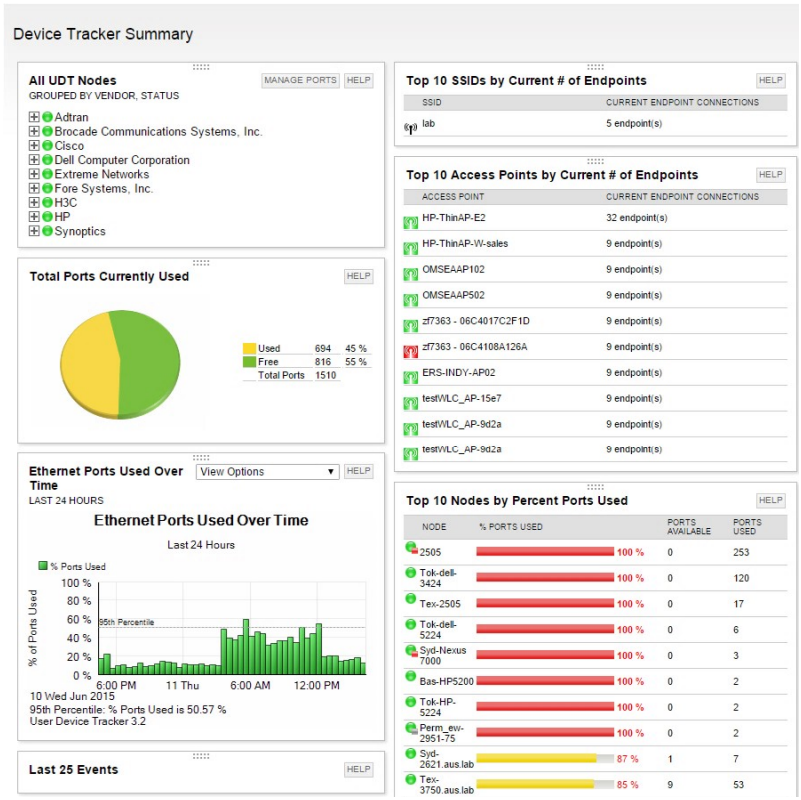


Figura 2.8: Interface de monitorização da ferramenta *User Device Tracker* [20].

Desta sumária análise do mercado, é possível identificar o interesse e a necessidade da realização de uma ferramenta de gestão e monitorização centralizada, *open source*, que permita a interoperabilidade entre os vários equipamentos de diferentes fabricantes. Deste modo, a tarefa de manter a configuração consistente por todos os APs autónomos seria facilitada.

Capítulo 3

MIBs

Neste capítulo é feita a análise de algumas MIBs relacionadas com a gestão de equipamentos sem fios. Na primeira secção irão ser avaliadas as MIBs públicas: a MIB-II e a MIB IEEE802dot11. Posteriormente, serão objeto de análise as MIBs privadas dos fabricantes Cisco, D-Link e Aruba.

3.1 Análise das MIBs *standard*

As MIBs, tal como já foi referido anteriormente, são uma coleção estruturada de objetos, ou seja, de dados a serem geridos, de um determinado equipamento. Através da consulta destas MIBs é possível perceber as características do equipamento a ser gerido. As MIBs podem ser públicas ou privadas, sendo que as privadas contêm informações específicas para dispositivos de um determinado fabricante.

Assim sendo, e de modo a cumprir o requisito de acesso às informações dos APs independentemente do fabricante, foram analisadas, numa primeira fase, duas MIBs *standard*, ou seja, comuns a dispositivos sem fios:

- **MIB-II**: Esta MIB é implementada por todos os dispositivos que suportam o protocolo SNMP. A sua descrição está presente na norma RFC 1213 [21]. A MIB-II revela informações gerais de um dispositivo como o nome, a descrição, a localização de um equipamento, bem como as suas interfaces, entre outros detalhes.

- **MIB IEEE802dot11**: Esta MIB está estruturada de acordo com a norma IEEE 802.11 [1] sendo, desta forma, específica para APs. As informações de gestão retiradas são independentes do fabricante, divulgando informações específicas de um AP como por exemplo o canal em que está a operar, os SSIDs e, na versão mais recente, as estações associadas.

3.1.1 MIB-II

A MIB-II (evolução da MIB-I) deriva do ramo *mgmt(2)* da árvore dos objetos, tal como se pode verificar na Figura 3.2, e é, atualmente, de extrema importância, visto que todos os dispositivos geríveis através de SNMP deverão suportar esta MIB.

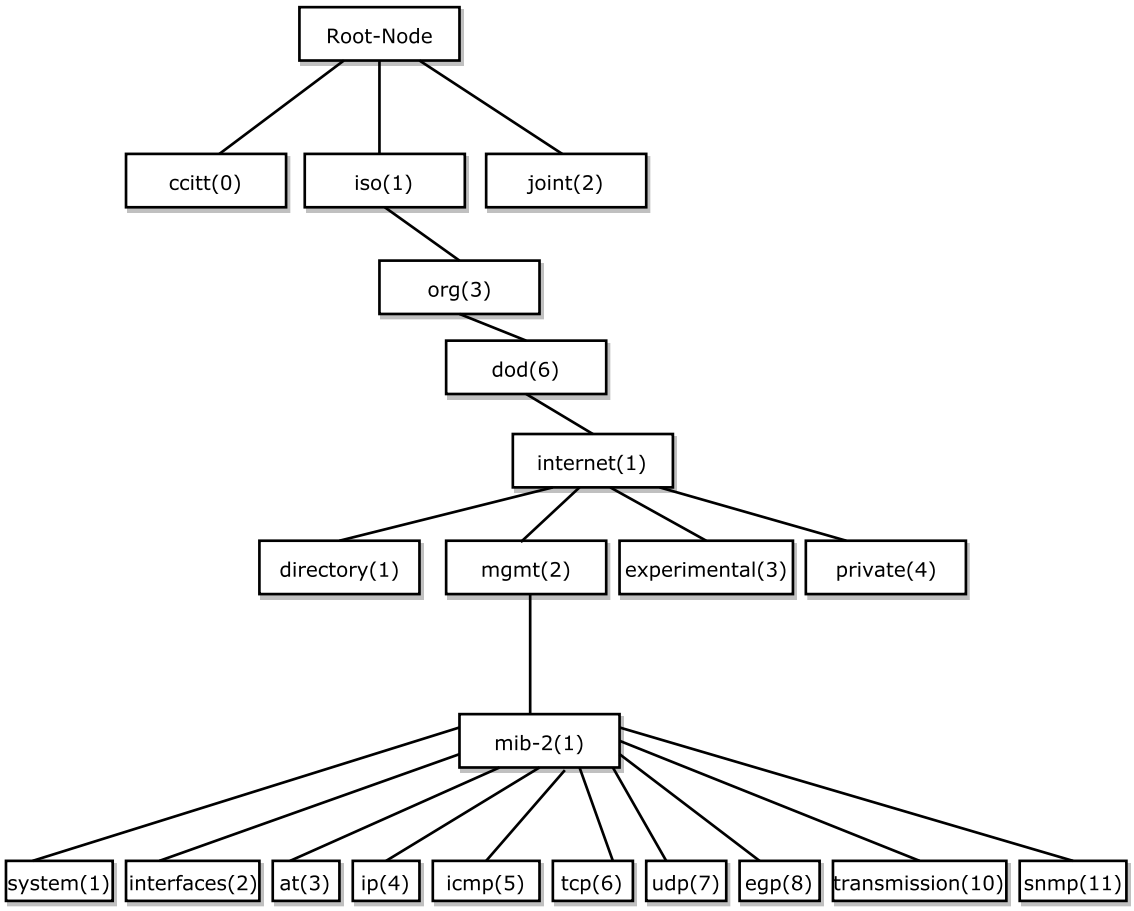


Figura 3.1: Árvore dos objetos contendo a MIB-II.

O ramo *system* apresenta uma lista de objetos pertencentes à operação do sistema. A partir deste ramo é possível retirar informações específicas de um dispositivo, como a sua descrição ou o seu OID, tal como se pode observar na tabela 3.1. Quando a permissão existente para um determinado objeto é *read-only*, este não se encontra ao alcance de modificações por parte do utilizador, enquanto que se a permissão existente for *read-write*, o utilizador já terá permissão para alterar o conteúdo do objeto. As permissões têm um maior impacto quando a gestão dos equipamentos envolve a alteração de configurações.

Objeto	Descrição	Permissões	OID
sysDescr	Contém uma descrição textual do sistema, incluindo o nome completo, as versões do *hardware* e *software* do dispositivo.	*Read-only*	1.3.6.1.2.1.1.1
sysObjectID	Retorna o OID do equipamento. Este valor é atribuído pelo fabricante, sendo possível perceber o tipo de sistema que se pretende gerir.	*Read-only*	1.3.6.1.2.1.1.2
sysUpTime	Disponibiliza a informação sobre o tempo decorrido desde que o sistema de gestão foi reinicializado.	*Read-only*	1.3.6.1.2.1.1.3
sysContact	Contém o contacto do proprietário do equipamento.	*Read-write*	1.3.6.1.2.1.1.4
sysName	Nome atribuído ao nó gerido.	*Read-write*	1.3.6.1.2.1.1.5
sysLocation	Descrição da localização do equipamento.	*Read-write*	1.3.6.1.2.1.1.6
sysServices	Indica, através do valor retornado, o conjunto de potenciais funcionalidades que o dispositivo oferece.	*Read-only*	1.3.6.1.2.1.1.7
sysORLastChange	Valor do objeto *sysUpTime* na altura em que existiu a alteração no estado mais recente.	*Read-only*	1.3.6.1.2.1.1.8
sysORTable	Tabela onde é feita a enumeração de funcionalidades da aplicação SNMP de acordo com as várias MIBs disponíveis.	*Read-only*	1.3.6.1.2.1.1.9

Tabela 3.1: Objetos do ramo *system* da MIB-II

No ramo *interfaces*, estão contidas as informações sobre todas as interfaces existentes no dispositivo, desde a sua descrição até ao seu estado de operação. Este ramo é composto por duas entradas: o *ifNumber* que indica o número total de interfaces existentes e *ifTable* - uma tabela que contém uma entrada com diferentes objetos para cada interface. Na tabela 3.2 é possível perceber o tipo de informação devolvida pela tabela das interfaces.

Objeto	Descrição	Permissões	OID
ifIndex	Índice único para cada interface, atribuído continuamente a partir de 1 até ao número de interfaces referenciado no *ifNumber*.	*Read-only*	1.3.6.1.2.1.2.2.1.1
ifDescr	Retorna a descrição de cada uma das interfaces, devendo conter o nome do fabricante, o nome do dispositivo e a versão do *hardware* e *software* da interface	*Read-only*	1.3.6.1.2.1.2.2.1.2
ifType	Indica o tipo da interface. Destacam-se o tipo 1 (other), o tipo 6 (ethernet), o tipo 71 (ieee80211) e o tipo 209 (bridge), para dispositivos que respeitem a norma IEEE 802.11	Read-only	1.3.6.1.2.1.2.2.1.3
ifMTU	Tamanho do maior pacote, em octetos, que poderá ser enviado ou recebido na interface em questão.	*Read-only*	1.3.6.1.2.1.2.2.1.4
ifSpeed	Estimativa da largura de banda da interface em bits/s. Para as interfaces cuja largura de banda não varie ou que não seja possível fazer uma estimativa, o objeto deverá conter o valor nominal.	*Read-only*	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	Endereço físico da interface, no caso dos APs trata-se do seu endereço MAC.	*Read-only*	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	O estado administrativo para a interface.	*Read-write*	1.3.6.1.2.1.2.2.1.7
ifOperStatus	Estado operacional atual da interface. Quando este objeto contém o valor 2 é porque a interface se encontra desligada. Caso o valor seja 1, a interface encontra-se ligada.	*Read-only*	1.3.6.1.2.1.2.2.1.8
ifLastChange	Valor do objeto *sysUpTime* no momento em que a interface alterou o seu estado operacional.	*Read-only*	1.3.6.1.2.1.2.2.1.9
ifInOctets	Número total de octetos recebidos numa interface.	*Read-only*	1.3.6.1.2.1.2.2.1.10

ifInUcastPkts	Número de pacotes recebidos, cuja entrega foi feita por uma camada superior com endereço *unicast*	*Read-only*	1.3.6.1.2.1.2.2.1.11
ifInNUCastPkts	Número de pacotes recebidos, cuja entrega foi feita por uma camada superior com endereço *multicast* ou *broadcast*. Este objeto foi substituído pelos objetos *ifInMulticastPkts* e *ifInBroadcastPkts*.	*Read-only*	1.3.6.1.2.1.2.2.1.12
IfInDiscards	Número de pacotes que foram descartados mesmo não contendo erros	*Read-only*	1.3.6.1.2.1.2.2.1.13
ifInErrors	Número de pacotes recebidos que contêm erros, impedidos de serem entregues a camadas superiores	*Read-only*	1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos	Número de pacotes recebidos e descartados por conterem um protocolo desconhecido ou não suportado.	*Read-only*	1.3.6.1.2.1.2.2.1.15
ifOutOctets	Número total de pacotes transmitidos a partir da interface.	*Read-only*	1.3.6.1.2.1.2.2.1.16
ifOutUCastPkts	Número total de pacotes transmitidos para uma camada superior e que não são endereçados para *broadcast* ou *multicast*.	*Read-only*	1.3.6.1.2.1.2.2.1.17
ifOutNUCastPkts	Número total de pacotes transmitidos para uma camada superior e que são endereçados para *broadcast* ou *multicast*.	*Read-only*	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	Número de pacotes entregues que foram descartados apesar de não conterem erros.	*Read-only*	1.3.6.1.2.1.2.2.1.19
ifOutErrors	Número de pacotes que não puderam ser enviados devido a erros.	*Read-only*	1.3.6.1.2.1.2.2.1.20
ifOutQLen	Comprimento da fila de saída de pacotes.	*Read-only*	1.3.6.1.2.1.2.2.1.21
ifSpecific	Referência às MIBs que contenham informações específicas para esta interface.	*Read-only*	1.3.6.1.2.1.2.2.1.22

Tabela 3.2: Objetos da tabela *ifTable* do ramo *interfaces* da MIB-II

Seguidamente, verifica-se a existência do ramo *at*, onde é feita a tradução do endereço IP em endereço físico (*Address Translation*). Este ramo está obsoleto e é utilizado apenas para a compatibilidade com versões anteriores [8]. Contém uma tabela com três objetos diferentes para cada interface mapeada. Apenas são contabilizadas as interfaces de dispositivos onde esta funcionalidade ainda se encontra ativa.

Objeto	**Descrição**	**Permissões**	**OID**
atIfIndex	Número da interface onde é possível fazer o mapeamento entre o endereço físico e o endereço de rede. O número da interface é equivalente ao valor do objeto *ifIndex* do ramo *interfaces*.	*Read-write*	1.3.6.1.2.1.3.1.1.1
atPhysAddress	Endereço físico da interface	*Read-write*	1.3.6.1.2.1.3.1.1.2
atNetAddress	Endereço de rede da interface	*Read-write*	1.3.6.1.2.1.3.1.1.3

Tabela 3.3: Objetos do ramo *at* da MIB-II

O ramo *ip* contém tabelas de endereços, tabelas de *routing*, e endereços de rede. Pode ser utilizado para se fazer *troubleshoot* aos problemas de uma rede. Contém, também, estatísticas de pacotes IP.

Dentro das várias informações obtidas por este ramo, é possível destacar o objeto *ipForwarding*, a tabela *ipAddrTable* e a tabela *ipNetToMediaTable*. O parâmetro *ipForwarding* indica se a entidade está a funcionar como um *router*, isto é, se está ou não a fazer o encaminhamento dos pacotes existentes.

O endereçamento da informação relevante para o endereço IPv4 de uma determinada entidade é feito na tabela *ipAddrTable*, representada em 3.4. Esta tabela encontra-se obsoleta visto ter sido adicionada uma nova, a *ipAddressTable*, onde a informação existente é independente da versão do endereço IP.

Objeto	Descrição	Permissões	OID
ipAdEntAddr	Endereço IP.	*Read-only*	1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex	Valor da interface correspondente a uma determinada entrada na tabela. Este valor é equivalente ao valor do objeto *ifIndex* do ramo *interfaces*.	Read-only	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	Máscara da *subnet* associada ao endereço IP.	Read-only	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	Valor do bit menos significativo do endereço de *broadcast* utilizado para enviar os datagramas na interface associada ao endereço IP desta entrada na tabela.	Read-only	1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize	Tamanho do maior datagrama IPv4 cujo equipamento consegue reordenar quando os recebe fragmentados nesta interface.	Read-only	1.3.6.1.2.1.4.20.1.5

Tabela 3.4: Objetos da tabela *ipAddrTable* do ramo *ip* da MIB-II

Por sua vez, a tabela *ipNetToMediaTable* 3.5, é utilizada para fazer o mapeamento entre o endereço IP e o respetivo endereço físico. Também esta tabela se encontra obsoleta, tendo sido substituída pela *ipAddressTable*.

Objeto	Descrição	Permissões	OID
ipNetToMediaIfIndex	Interface na qual vai ser feito o mapeamento. O valor deste parâmetro é equivalente ao valor do parâmetro *ifIndex* do ramo *interfaces*	*Read-create*	1.3.6.1.2.1.4.20.1.1
ipNetToMediaPhysAddress	Endereço físico da interface em questão.	*Read-create*	1.3.6.1.2.1.4.20.1.2
ipNetToMediaNetAddress	Endereço IP correspondente à interface em questão.	*Read-create*	1.3.6.1.2.1.4.20.1.3
ipNetToMediaType	Tipo de mapeamento.	*Read-create*	1.3.6.1.2.1.4.20.1.4

Tabela 3.5: Objetos da tabela *ipAddrTable* do ramo *ip* da MIB-II

No ramo *icmp* é possível obter estatísticas sobre mensagens ICMP (*Internet Control Message Protocol*) tais como o número de mensagens enviadas e recebidas pelo dispositivo, número total de mensagens recebidas, enviadas, recebidas com erros ou não enviadas devido a limitações de

recursos. Neste ramo apenas as tabelas *icmpStatsTable* e *icmpMsgStatsTable* não se encontram obsoletas.

Os ramos *tcp* e *udp* apresentam o estado de conexão de cada um dos protocolos de transporte, bem como parâmetros, estatísticas e tráfego associado.

As estatísticas e o tráfego do protocolo EGP (*Exterior Gateway Protocol*) são informações apresentadas pelo ramo *egp*.

No ramo *transmission* não são definidos objetos. É um ramo que serve de raíz para outras MIBs com objetos específicos.

Por fim, o ramo *snmp* apresenta as estatísticas do tráfego do protocolo SNMP, contendo objetos que permitem perceber o nível de utilização do agente, que tipo de erros é que o agente consegue captar e a quantidade de tráfego SNMP que está a ser gerada na rede.

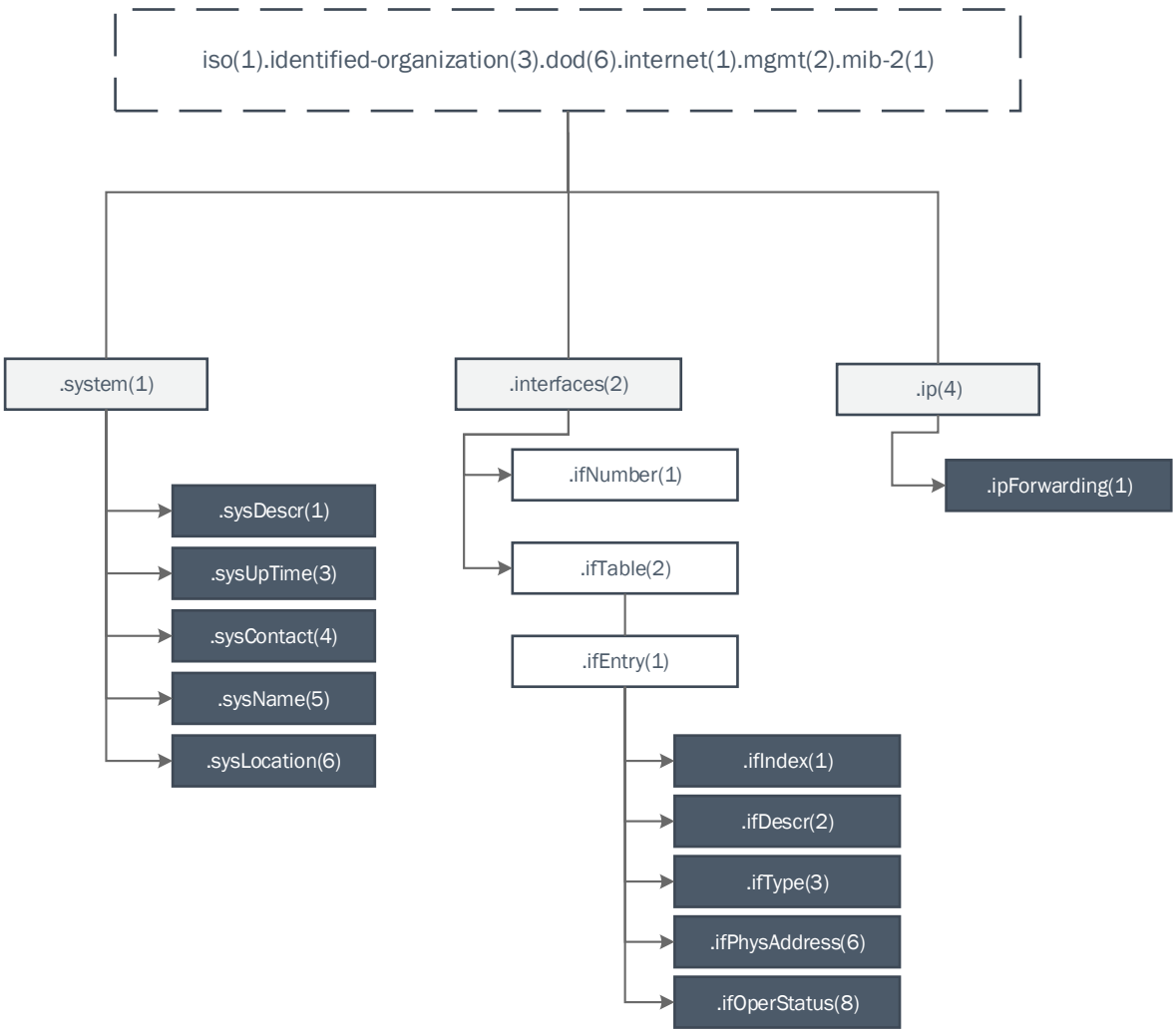


Figura 3.2: Parâmetros da MIB-II fundamentais para o desenvolvimento do projeto.

3.1.2 MIB IEEE 802.11

A MIB IEEE802dot11 é uma MIB destinada a gerir equipamentos compatíveis dentro da norma 802.11 do IEEE e está localizada no ramo 1.2.840.10036. Esta MIB disponibiliza duas versões: uma de 2003, ainda muito utilizada em diversos equipamentos e outra mais recente, a versão de 2012.

Esta MIB é composta por sete ramos:

- **dot11smt(1)**: contém objetos que permitem disponibilizar informação para gerir estações Wi-Fi.

  Este ramo é dedicado à gestão das estações e é composto por 26 grupos, na sua maioria tabelas, onde é possível retirar informações sobre as configurações de uma estação Wi-Fi, os algoritmos de autenticação e de segurança do equipamento, notificações, mobilidade, opções de gestão e configuração de estações pertencentes a uma rede *Mesh* (topologia de rede distribuída).

  Na tabela *dot11StationConfigTable* é possível obter-se a identificação da estação (o seu endereço MAC), a configuração dos *timeouts* e as opções de segurança implementadas. Em relação à versão da MIB de 2003, esta tabela, agora atualizada, contém um maior número de parâmetros incluindo informações sobre o espectro, a implementação do algoritmo de autenticação RSNA (*Robust Security Network Association*), a possibilidade de utilização de ACKs (*Acknowledgements*) durante a transmissão e detalhes das estações associadas ao dispositivo. A tabela *dot11AuthenticationAlgorithmsTable* apresenta os algoritmos de autenticação suportados pelas estações contendo as opções de *Open System*, *Shared Key*, FT (*Fast BSS Transition*) e SAE (*Simultaneous Authentication of Equals*). Também as informações de gestão relacionadas com a gestão do espetro e potência se encontram presentes neste ramo. A localização do equipamento e a coexistência de vários SSIDs são informações com grande utilidade e que podem ser consultadas em *dot11WirelessMgmtOptionsTable*.

- **dot11mac(2)**: providencia informação para o controlo de acesso - camada MAC. Contém três tabelas relacionadas com parâmetros de operação como *timeouts*, *retries*, contadores e fragmentação de tramas. É também possível aceder às informações inerentes ao equipamento: a identificação do fabricante, a partir do objeto *dot11ManufacturerID* e a identificação do produto - *dot11ProductID*.

- **dot11res(3)**: disponibiliza informação sobre a interface rádio da estação a gerir como o OUI (*Organizationally Unique Identifier*) do fabricante ou o nome e versão da interface.

- **dot11phy(4)**: este ramo contém informação para a gestão da camada física da interface de rede da estação. Aqui são identificados os aspetos relacionados com a camada física: tipo, detalhes relacionados com as antenas como a potência enviada e recebida e os canais existentes. Também contém objetos que abordam a técnica de espalhamento de espetro por salto em frequência (FHSS) e a técnica de espalhamento de espectro por sequência direta (DSSS).

- **dot11Conformance(5)**: ramo composto por grupos de objetos semelhantes entre si ou com a mesma finalidade de gestão.
- **dot11imt(6)**: providencia o suporte necessário para a gestão e interoperabilidade entre diferentes sistemas. Na tabela *dot11BSSIdTable* é possível encontrar o objeto *APMacAddress*, que indica o endereço MAC do AP.
- **dot11MSGCF(7)**: contém informações sobre eventos acionados para protocolos de camadas superiores e as capacidades para suportar esses eventos;

É possível identificar uma grande diferença entre as duas versões desta MIB: a versão de 2003 ainda não contém os ramos *dot11imt(6)* e *dot11imt(7)*, adicionados posteriormente em 2012.

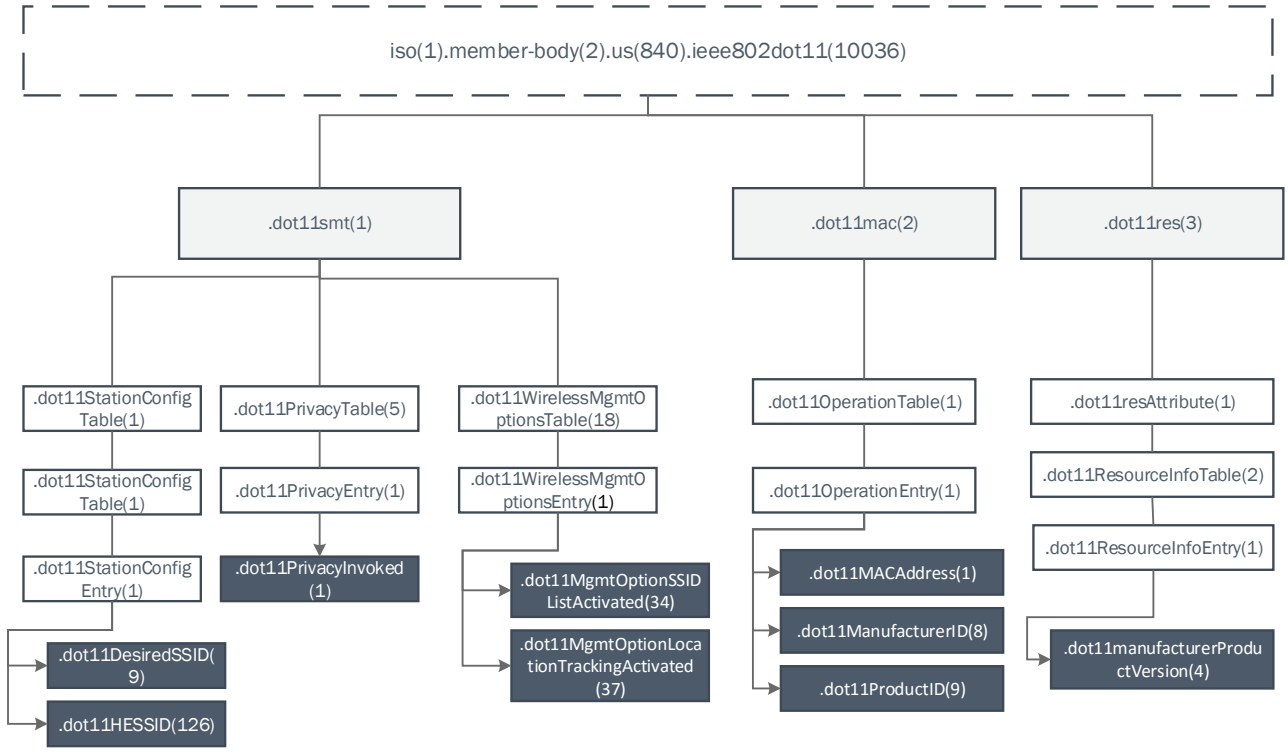


Figura 3.3: Ramos *dot11smt(1)*, *dot11mac(2)*, *dot11res(3)* da MIB IEEE802dot11 e alguns dos objetos fundamentais para a gestão de uma infraestrutura de rede Wi-Fi.

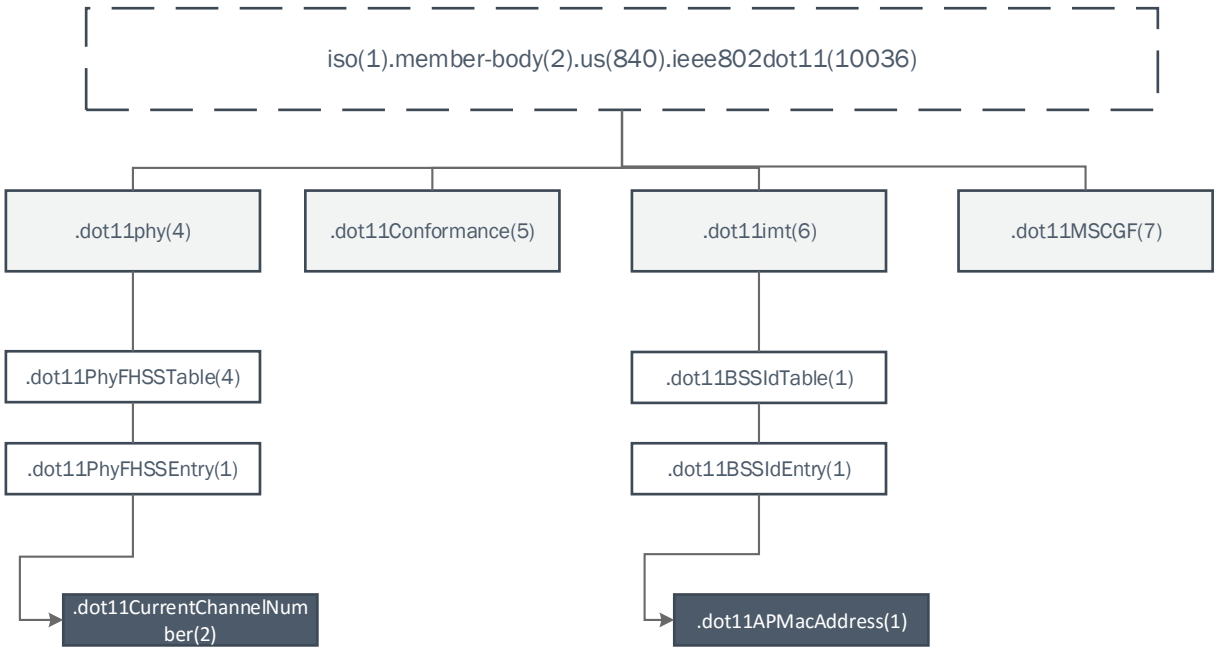


Figura 3.4: Ramos *dot11phy(4)*, *dot11Conformance(5)*, *dot11imt(6)* e *dot11MSGCF(7)* da MIB IEEE802dot11 ee alguns dos objetos fundamentais para a gestão de uma infraestrutura de rede Wi-Fi.

3.2 Análise das MIBs privadas

Para a elaboração deste projeto foi necessário ter em conta as MIBs privadas dos equipamentos e perceber quais as informações relevantes adicionais que estas MIBs apresentam. Assim sendo, nesta secção irão ser abordadas as MIBs privadas dos fabricantes Cisco, D-Link e Aruba.

3.2.1 Cisco

A MIB desenvolvida pela Cisco para monitorar e gerir os seus equipamentos subdivide-se em 20 ramos, sendo o ramo *ciscoMgmt (9)* utilizado para o desenvolvimento de novas MIBs, contendo também os principais objetos relacionados com a norma IEEE 802.11 situados nas seguintes MIBs:

- CISCO-DOT11-IF-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DOT11-SSID-SECURITY-MIB

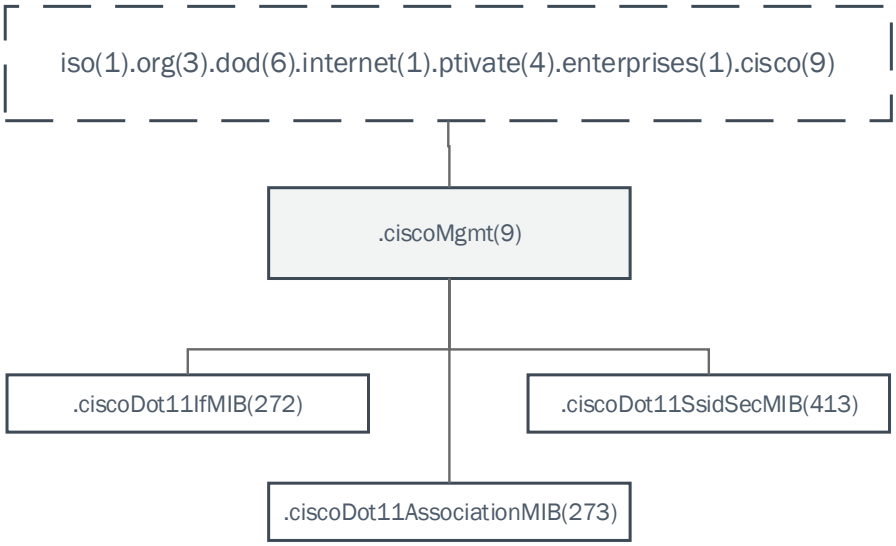


Figura 3.5: As três MIBs do fabricante Cisco fundamentais para a gestão de uma infraestrutura de rede sem-fios

3.2.1.1 CISCO-DOT11-IF-MIB

As informações da CISCO-DOT11-IF-MIB podem ser obtidas pelo OID 1.3.6.1.4.1.9.9.272. Esta MIB proporciona um apoio à gestão das interfaces rádio dos APs Cisco.

Através desta MIB é possível obter informações sobre as estações associadas como o número máximo e o respetivo endereço MAC (*cd11IfAddignedSTA*), os SSIDs (*cd11IfAuxSsid*), as VLANs existentes (*cd11IfAuxSsidAuthAlgDefaultVlan*), e o modo de operação do AP (*cd11IfPhyMacSpecification*). A indicação se o SSID se encontra ou não em *broadcast* é obtida pelo objeto *cd11IfAuxSsidAuthAlgEnable*.

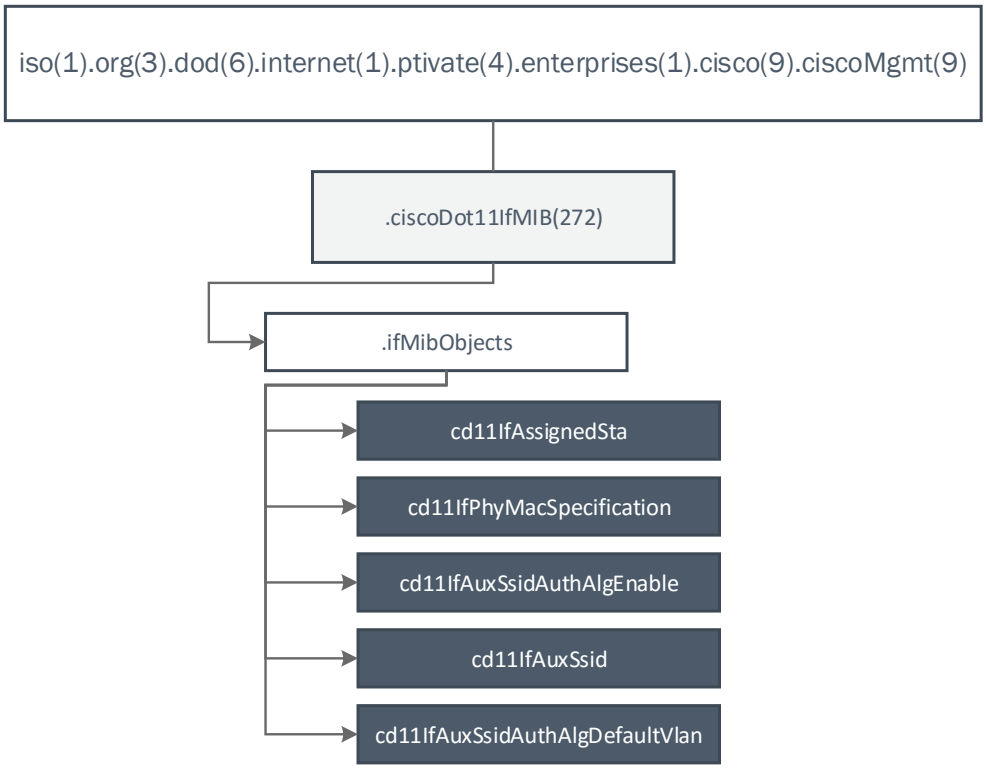


Figura 3.6: Principais objetos para a gestão das interfaces rádio dos APs Cisco contidos na MIB CISCO-DOT11-IF-MIB.

3.2.1.2 CISCO-DOT11-ASSOCIATION-MIB

Os objetos necessários para a gestão da associação entre equipamentos Wi-Fi, como as estatísticas, o reencaminhamento de pacotes e as configurações das estações, poderão ser encontrados na MIB CISCO-DOT11-ASSOCIATION-MIB, através do OID 1.3.6.1.4.1.9.9.273. Nesta MIB é apresentada a informação por estação, sendo esta uma extensão à MIB IEEE802dot11.

O número de estações associadas a um AP (*cDot11ActiveWirelessClients*), o seu endereço IP (*cDot11ClientIPAddress*) e o tipo de equipamento (*cDot11ClientDevType*) são informações necessárias para a gestão de uma infraestrutura de rede Wi-Fi e que podem ser encontradas nesta MIB.

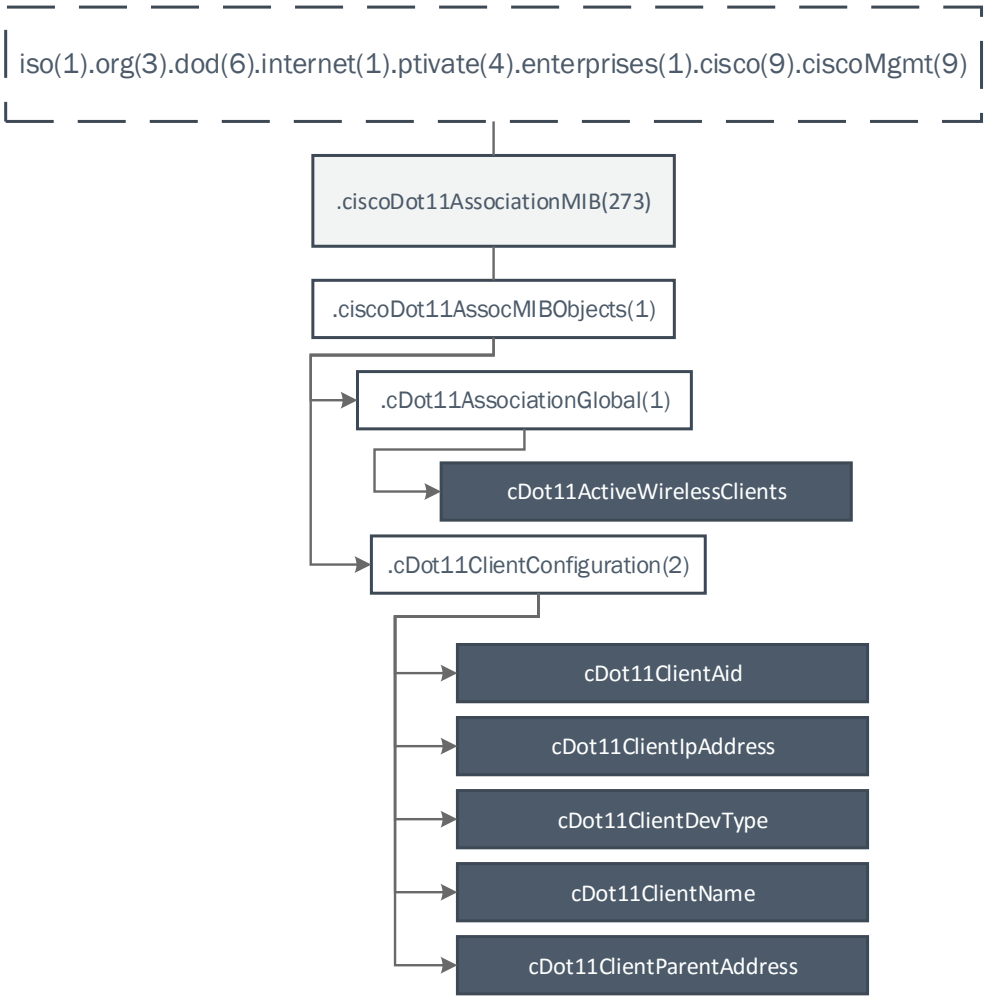


Figura 3.7: Estrutura e objetos fundamentais presentes na MIB CISCO-DOT11-ASSOCIATION-MIB.

3.2.1.3 CISCO-DOT11-SSID-SECURITY-MIB

A MIB CISCO-DOT11-SSID-SECURITY-MIB providencia um suporte para a gestão da rede, na área da associação e autenticação das estações. Contém informações importantes sobre os SSIDs existentes. É possível perceber a partir desta MIB se o AP contém um ou múltiplos SSIDs (*cdot11SecAuxSsidAuthEnabled*), bem como os seus respetivos BSSID (*Basic Service Set IDentifier*): *cdot11MbssidIfMacAddress* e os BSSIDs suportados pelo equipamento (*cdot11MbssidMacAddrSupported*).

Esta MIB encontra-se presente no OID 1.3.6.1.4.1.9.9.413.

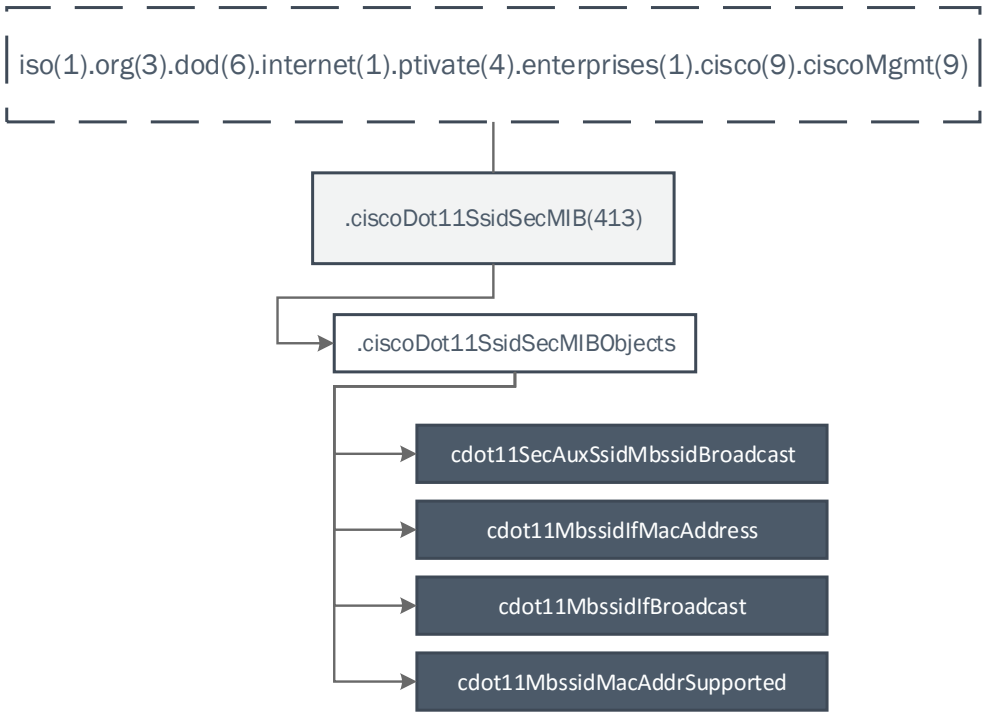


Figura 3.8: Estrutura e objetos fundamentais presentes na MIB CISCO-DOT11-SSID-SECURITY-MIB.

3.2.2 D-Link

O fabricante D-Link desenvolveu uma MIB privada para a gestão dos seus APs denominada AP-config e que se situa no OID 1.3.6.1.4.1.171.11.37.4. Apesar do nó dentro do ramo *dlink-mgmt (11)* ter o nome de um AP específico deste fabricante: *dwl2100AP*, esta MIB é comum a vários modelos de APs da D-Link.

Esta MIB contém cinco ramos:

- **home (1)**: este ramo é composto por duas tabelas. A tabela *hWirelessBandTable* que divulga informações sobre a interface *wireless*, como o SSID, o canal utilizado para a transmissão e os canais disponíveis. O endereço IP do equipamento, a máscara e a *default gateway* estão presentes na tabela *hLan*.

- **advanced (2)**: os parâmetros relativos ao modo em que o equipamento está a operar, a configuração dos objetos da interface rádio, segurança, encriptação e DHCP (*Dynamic Host Configuration Protocol*) encontram-se presentes neste ramo. Aqui também será possível aceder a informações relativamente à existência de múltiplos SSIDs e VLANs, servidor TFTP (*Trivial File Transfer Protocol*), *logfiles* e tipo de BSS configurado.

- **tools (3)**: este ramo é composto por quatro tabelas que revelam detalhes relacionados com a administração do AP: configurações de *usernames* e *passwords*, protocolo SNMP, gama de IPs, definições de fábrica, servidor TFTP, *updates* e versões de *firmware*.

- **status (4)**: tal como o nome indica, neste ramo estão presentes informações sobre o estado do AP: endereço MAC e IP, o SSID principal, o canal e outras informações relativas à interface rádio. Também é possível obter detalhes sobre os clientes associados ao AP como o seu endereço MAC, o tipo de autenticação, o tipo de estação e qual o SSID onde a estação se encontra conectada.

- **functionality (99)**: contém objetos sobre o modo do AP, o código do país e as funcionalidades ativas no equipamento.

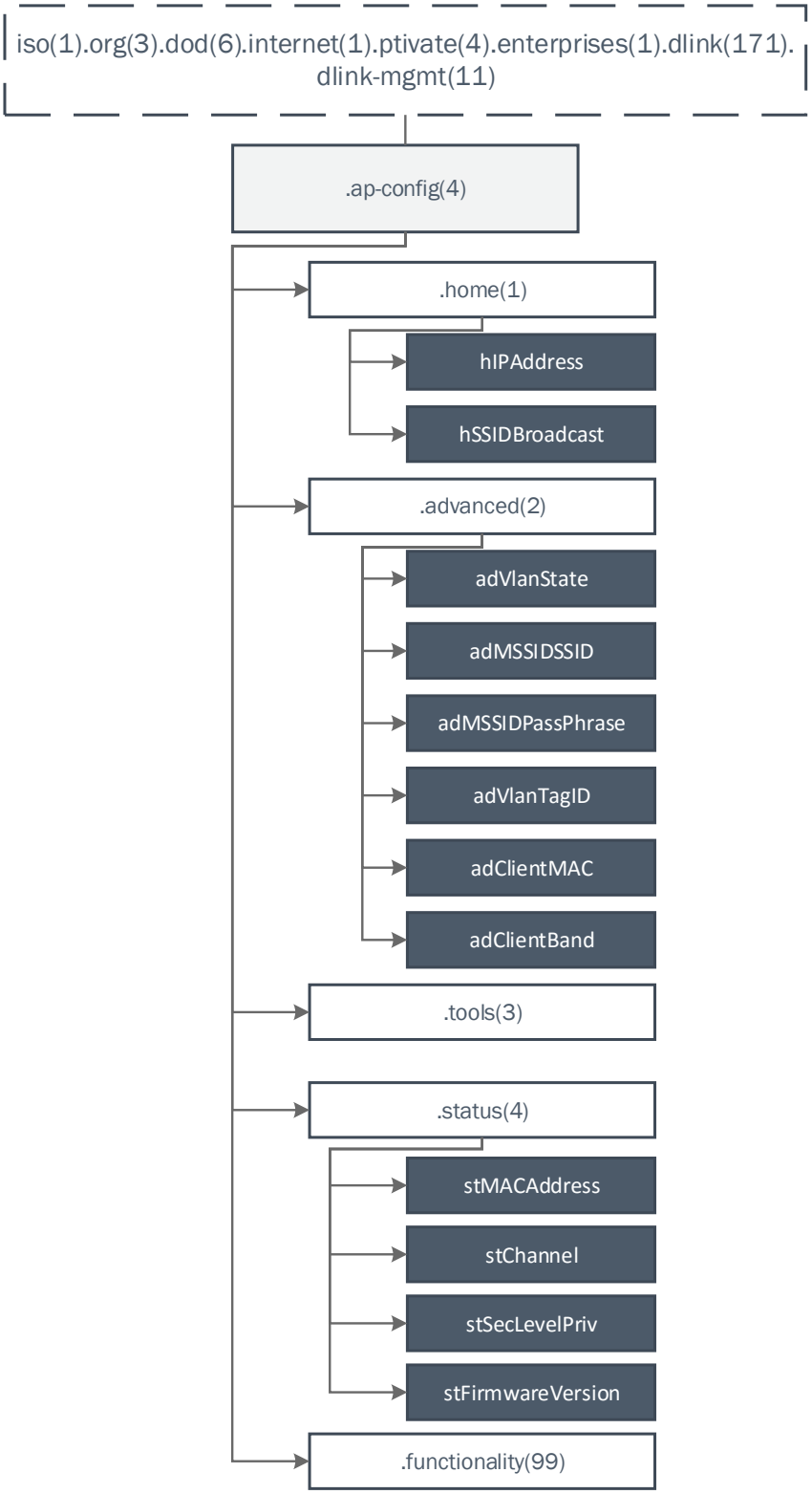


Figura 3.9: Estrutura e objetos fundamentais presentes na MIB privada do fabricante D-Link.

3.2.3 Aruba

O fabricante Aruba desenvolveu uma MIB com o objetivo de gerir os seus APs: a Aruba Instant MIB (aiMIB), presente no OID 1.3.6.1.4.14823.2.3.3.

Esta MIB é composta por dois ramos. O ramo *aiInfoGroup* e o ramo *aiStateGroup* que é composto por quatro tabelas:

- **aiAccessPointTable**: contém informação mais geral sobre o AP em questão, como o endereço MAC, o modelo do equipamento, o número de série e a sua versão.
- **aiRadioTable**: disponibiliza detalhes por cada interface rádio existente no AP: desde o endereço MAC, a potência do sinal transmitido e do ruído, bem como o canal em que opera.
- **aiWlanTable**: contém informação sobre todos os BSSIDs ativos, os seus endereços, o número de tramas recebidas e enviadas, e os SSIDs existentes.
- **aiClientTable**: apresenta os objetos relativos às estações associadas ao AP: número de equipamentos conectados, os seus endereços MAC e IP, o nome dos dispositivos e os SSIDs onde se encontram conectados. É também possível obter informações sobre o número de bytes transmitidos e recebidos pelo cliente.

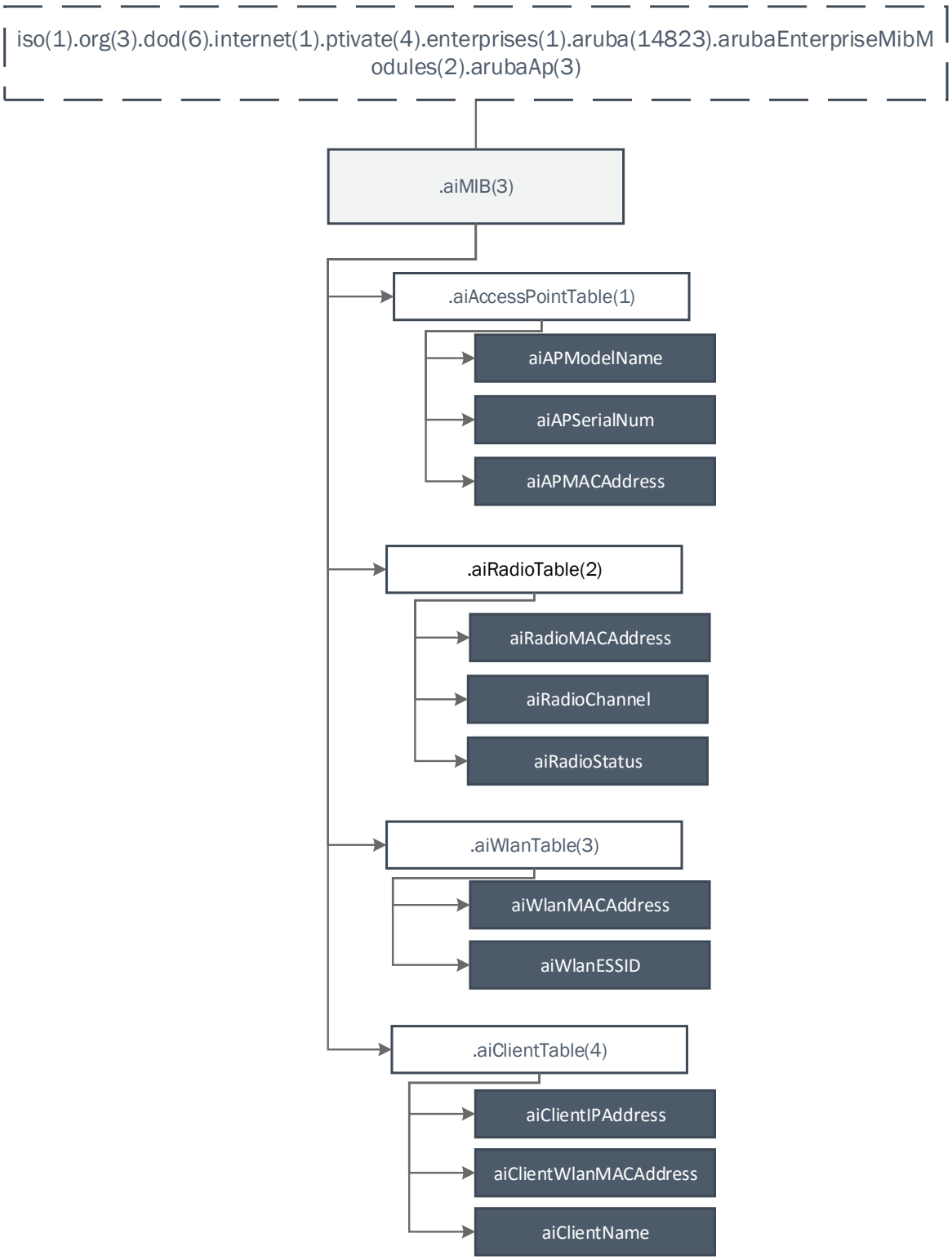


Figura 3.10: Estrutura e objetos fundamentais presentes na MIB privada do fabricante Aruba.

Capítulo 4

Solução Proposta

Neste capítulo é apresentada a solução proposta para a resolução do problema. É apresentada, em primeiro lugar, a arquitetura da solução onde são enumeradas as tecnologias e equipamentos utilizados. Seguidamente é descrita a implementação desta solução, composta pela pesquisa de rede, acesso às configurações dos APs e a alteração dessas configurações, desenvolvimento da base de dados e da interface gráfica. Por fim, é exposta a validação da solução.

4.1 Arquitetura da solução

A imagem 4.1 demonstra a arquitetura utilizada no desenvolvimento deste projeto.

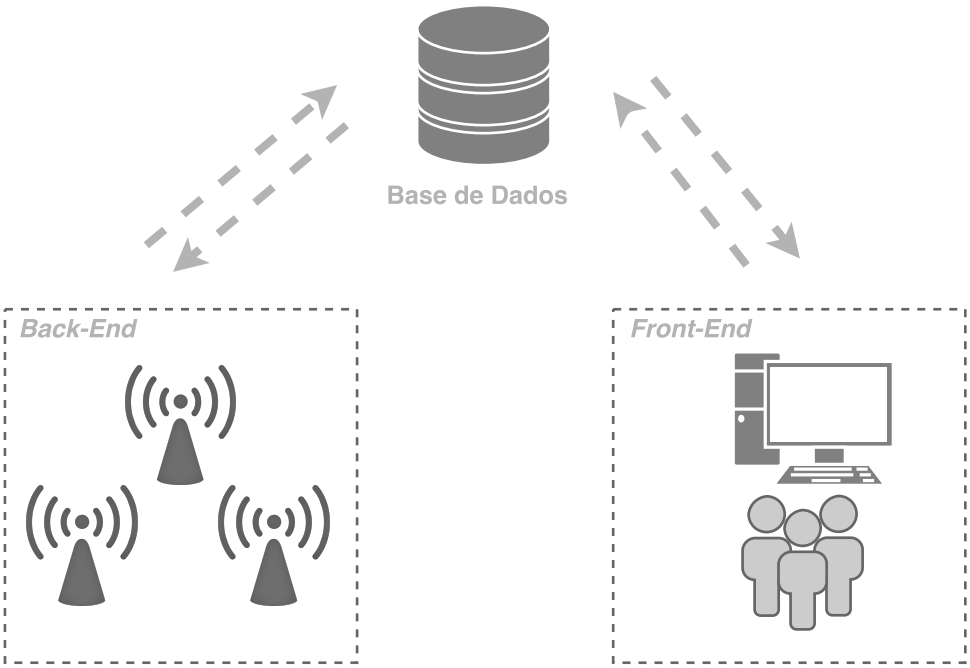


Figura 4.1: Arquitetura da solução.

Nesta topologia é possível identificarmos dois conjuntos de tarefas distintos: o *back-end*, responsável pela leitura e escrita de informação nos APs e o *front-end* onde é feita toda a comunicação com o utilizador. O *back-end* e o *front-end* partilham uma base de dados única.

O utilizador, quando pretende receber informações sobre os APs existentes numa determinada rede ou numa gama de endereços IP, ou alterar configurações, insere as informações necessárias no campo de pesquisa enviando, assim, um pedido que é redirecionado para a base de dados.

No *back-end*, existe um *script* que é executado de minuto em minuto, verificando na base de dados se existe algum pedido de pesquisa ou alteração de parâmetros. Consoante as ordens que recebe, reencaminha o pedido para os módulos que fazem a comunicação com o AP através do protocolo SNMP. Depois de executado o pedido, seja de leitura ou de escrita, o *back-end* envia as informações finais dos APs, interfaces, SSIDs e estações existentes na rede em questão.

Por fim, a interface *web* acede sempre aos dados mais recentes e atualizados da base de dados, exibindo os dados ao utilizador.

Esta arquitetura tem a vantagem de o *front-end* apenas estar dependente da base de dados, apresentando sempre ao utilizador os dados atualizados. O *back-end* acaba por ser o motor do projeto, onde é feita a pesquisa da rede e a comunicação com o AP. Como ambos comunicam com uma base de dados comum, é possível separar fisicamente o *back-end* do *front-end*, permitindo uma maior mobilidade, acabando por ser também uma mais valia ao nível da organização e da escalabilidade durante o desenvolvimento do projeto.

4.1.1 Tecnologias utilizadas na implementação da solução

Na implementação da solução foram utilizadas diferentes tecnologias:

- Net-SNMP como ferramenta para o protocolo SNMP devido ao facto de implementar um agente SNMP e de existirem bibliotecas em várias linguagens de programação para a análise do conteúdo dos equipamentos;

- PHP como linguagem de programação dos módulos de acesso aos APs e de interação com o utilizador, por ter bibliotecas específicas e relacionadas com a interface *web* a desenvolver. Foi também escolhida esta linguagem pelo facto de conter bibliotecas de acesso à ferramenta Net-SNMP que permitem gerir remotamente os equipamentos utilizando o protocolo SNMP, bem como MySQL, responsáveis pela conexão com a base de dados e também o envio e receção de dados;

- *Framework* Bootstrap para o desenvolvimento da interface gráfica;

- Nmap, como ferramenta de pesquisa de rede, por ser flexível, permitindo realizar a pesquisa da rede através da verificação de portas;

- Servidor de base de dados MySQL, devido à sua robustez e desempenho;

- Servidor *Web* Apache, visto ser até ao momento o servidor mais utilizado no mundo para este fim, contendo uma excelente *performance*, segurança e compatibilidade com diversas plataformas.

4.1.2 Equipamentos utilizados para testes na implementação da solução

Durante a implementação da solução foram utilizados diferentes APs autónomos para a realização de testes. Na tabela 4.1 são apresentados os APs utilizados e o modo como irão ser referenciados ao longo desta dissertação.

Modelo do Equipamento	**Referência ao longo da dissertação**
Cisco Aironet 1100	AP Cisco 1100
D-Link DWL-2100	AP D-Link
Cisco Aironet 1200	AP Cisco 1200
TP-Link TL-WR841N/ND	AP TP-Link
Aruba IAP-225	AP Aruba

Tabela 4.1: APs utilizados para a realização de testes

Os APs Cisco e o AP D-Link contêm apenas uma interface rádio na gama dos 2.4 GHz seguindo a norma IEEE 802.11g. O AP TP-Link, também contém uma interface rádio na gama dos 2.4 GHz mas já integra a norma IEEE 802.11n. Por fim, o AP Aruba é *dual radio*, estando presente na banda dos 2.4 GHz e 5 GHz, suportando a norma IEEE 802.11n e 802.11ac.

O AP TP-Link com o seu *software* inicial não previa o acesso ao protocolo SNMP. Sem essa característica, não seria possível integrá-lo nos testes do projeto. Para ultrapassar esta limitação foi feita a instalação de um novo *software* neste equipamento: o OpenWRT.

O OpenWRT é um sistema operativo embutido, *open-source*, baseado em Linux. Permite instalar pacotes, como o snmpd, de um repositório de *software*. É possível aceder e configurar o equipamento através do terminal, por SSH (*Secure Shell*), ou através de uma interface gráfica (LuCI). O OpenWRT encontra-se disponível para vários modelos de AP.

No caso do AP TP-Link, a instalação deste software e do pacote snmpd, tornaram possível o acesso às informações disponibilizadas pela MIB IEEE802dot11 na versão de 2003. Veio-se, também, a verificar que a MIB do fabricante TP-Link não se encontrava implementada, não sendo possível deste modo ter acesso às informações das estações conectadas. Para além deste inconveniente, também se verificou que sempre que é adicionado um novo SSID, o novo endereço MAC criado é uma cópia do original mas com o primeiro octeto do endereço alterado, em vez do último. Este é um erro grave desta configuração, pois uma alteração no primeiro octeto afeta o OUI do equipamento, transmitindo informações erradas sobre o fabricante do AP.

O AP D-Link apresenta também algumas configurações erradas, apresentando o mesmo endereço MAC para as interfaces *Ethernet* e rádio, estando o parâmetro *ifOperStatus* da MIB-II sempre

ativo, mesmo que a interface se encontre desligada. Após um teste, utilizando o AP como *repeater*, para se conseguir perceber o verdadeiro endereço MAC da interface rádio, constatou-se que este endereço foi gerado a partir do AP de onde se queria repetir o sinal, tal como se pode verificar pela tabela 4.2.

Equipamento	**Endereço MAC da interface rádio**
AP base	00:12:D9:42:95:90
D-Link em modo AP	00:0E:83:BC:C4:B0
D-Link em modo *repeater*	00:0E:D9:42:95:90

Tabela 4.2: Teste do AP D-Link em modo *repeater*

A deteção, resolução e uniformização destas inconsistências nos APs utilizados, revelaram-se uma das principais dificuldades do projeto.

O AP Aruba é o único AP *dual radio* utilizado para testes. Já não foi possível utilizar este AP para a elaboração de testes durante a fase da construção dos módulos da alteração de configurações. Contudo, foram desenvolvidos os módulos de acesso às suas informações. Este AP tem a particularidade de demorar no mínimo cerca de 1 minuto a limpar as configurações, sendo necessário contabilizar esse tempo na sincronização da informação.

4.2 Implementação

4.2.1 Pesquisa da Rede

Um dos requisitos para uma gestão eficiente é a implementação de uma pesquisa de rede automática que permita, numa qualquer infraestrutura de rede, diferenciar os APs ligados e geríveis, dos restantes equipamentos como *routers*, *switches* ou mesmo computadores com placas de rede sem fios. Esta distinção não é possível fazer diretamente através das MIBs dos APs, daí ter sido desenvolvido um algoritmo de pesquisa da rede.

Para isso, recorreu-se à ferramenta Nmap para se identificar os equipamentos ligados e com a porta utilizada nas comunicações SNMP, a porta 161, aberta. O Nmap é uma ferramenta gratuita e open-source para a descoberta dos componentes da rede.São utilizados pacotes IP para determinar quais os *hosts* disponíveis e quais os serviços que estes oferecem.

Para se realizar a pesquisa é necessário indicar a rede com a máscara de *subnet* ou apenas um endereço IP e as definições da pesquisa, neste caso pesquisa em TCP e UDP na porta 161. Esta chamada para a ferramenta Nmap é feita com recurso uma função que permite executar um comando através da *shell* e retorna o resultado como uma *string*. Codificando a *string* no formato xml, é possível obterem-se os endereços IP para os quais o resultado do estado da porta 161 é *open*.

Obtidos os endereços IP dos equipamentos potencialmente geríveis e ligados, é necessário identificar os APs seguindo uma série de rotinas, visto nem todos conterem a MIB IEEE802dot11 implementada. Em condições ideias apenas seria necessário testar um objeto existente nesta MIB para se identificarem, à partida, todos os APs existentes numa rede.

Assim sendo, é necessário determinar se a *community* inserida pelo utilizador está correta e distinguir os *routers* dos restantes. Para isso, é utilizado o objeto *ipForwarding* da MIB-II que indica se os pacotes estão ou não a ser reencaminhados no equipamento. Caso estejam a ser reencaminhados, encontramo-nos perante um *router*, descartando-se esse endereço IP.

Seguidamente analisam-se as interfaces dos equipamentos restantes, para tentar identificar, através da descrição, se estes contêm uma interface rádio. A identificação da interface rádio é feita através da descrição, devido ao parâmetro *ifType* da MIB-II não estar, por vezes, em alguns APs bem implementado. Às interfaces rádio deveria estar associado um valor diferente de 6 (*ethernet*), preferencialmente 71 (*ieee80211*), mas em APs como no D-Link retorna o valor 1 (*other*) ou mesmo como no TP-Link que retorna o valor 6. Também as informações acerca do *speed* aliadas ao MTU (*Maximum Transmission Unit*) acabam por ser inconclusivas, visto não serem constantes entre APs. Uma outra possibilidade seria a verificação da existência da Bridge-MIB para comprovar a existência de uma interface rádio. Depois de alguns testes foi possível concluir que esta MIB não existe na maioria dos APs em teste, à semelhança da MIB IEEE802dot11. Outro critério poderia ser o facto do endereço MAC da interface rádio ser diferente do endereço MAC da interface Ethernet, não se verificando, estranhamente, esta premissa no AP D-Link.

A identificação da interface rádio é necessária para, em primeiro lugar, rejeitar todo os dispositivos, que não a possuam e também para a identificação do fabricante, decisiva para a posterior

escolha das MIBs a utilizar. É também, pela identificação do fabricante ser feita a partir destas interfaces, que não se podem utilizar parâmetros das MIBs privadas para a sua identificação.

No caso de não se estar perante uma interface rádio, esses dispositivos serão descartados, os restantes poderão ser APs mas poderão ser, também, placas de rede inseridas em computadores, por exemplo. Deste modo, em segundo lugar, é feita a seleção dos primeiros três octetos do endereço MAC, de forma a permitir identificar o fabricante. Esta identificação é feita através da comparação do resultado com os três primeiros octetos dos fabricantes de APs existentes, presentes num documento disponibilizado pelo IEEE [22]. Se o fabricante não pertencer a essa lista, o equipamento é retirado da lista de possíveis APs.

A condição seguinte serve para verificar se o equipamento contém a MIB IEEE802dot11 instalada, recorrendo a uma chamada SNMP com o objeto que traduz o BSSID. O BSSID foi o parâmetro escolhido visto ser um dos parâmetros implementados por todos os APs em teste dentro dessa MIB. Caso a resposta seja afirmativa, é seguro afirmar que se está perante um AP e que é possível utilizar os módulos desenvolvidos com essa MIB *standard* para o acesso aos APs.

Caso a resposta seja negativa, é feita uma chamada SNMP à MIB privada do fabricante em questão. Neste caso, se existir resposta, é feita a verificação da existência de módulos desenvolvidos de acesso ao AP de acordo com esse fabricante. É também verificada a existência de SSID para se descartar a possibilidade de não se estar perante um AP, de ser, por exemplo, uma placa de rede de um computador desenvolvido por um fabricante que também se insere na indústria dos APs. Caso não existam módulos, visto só terem sido desenvolvidos os necessários para os APs em teste, há sempre a possibilidade de os desenvolver e de os adicionar ao projeto, tornando-o escalável.

O tempo de pesquisa da rede varia consoante o tamanho da rede a pesquisar, mas é esta a parte mais demorada de todos os processos do *back-end*. Isto poderá dever-se ao facto de, com a ferramenta Nmap, ser verificado um IP de cada vez e de poderem existir equipamentos na rede ligados, com o protocolo SNMP ativo, mas com uma *community* diferente.

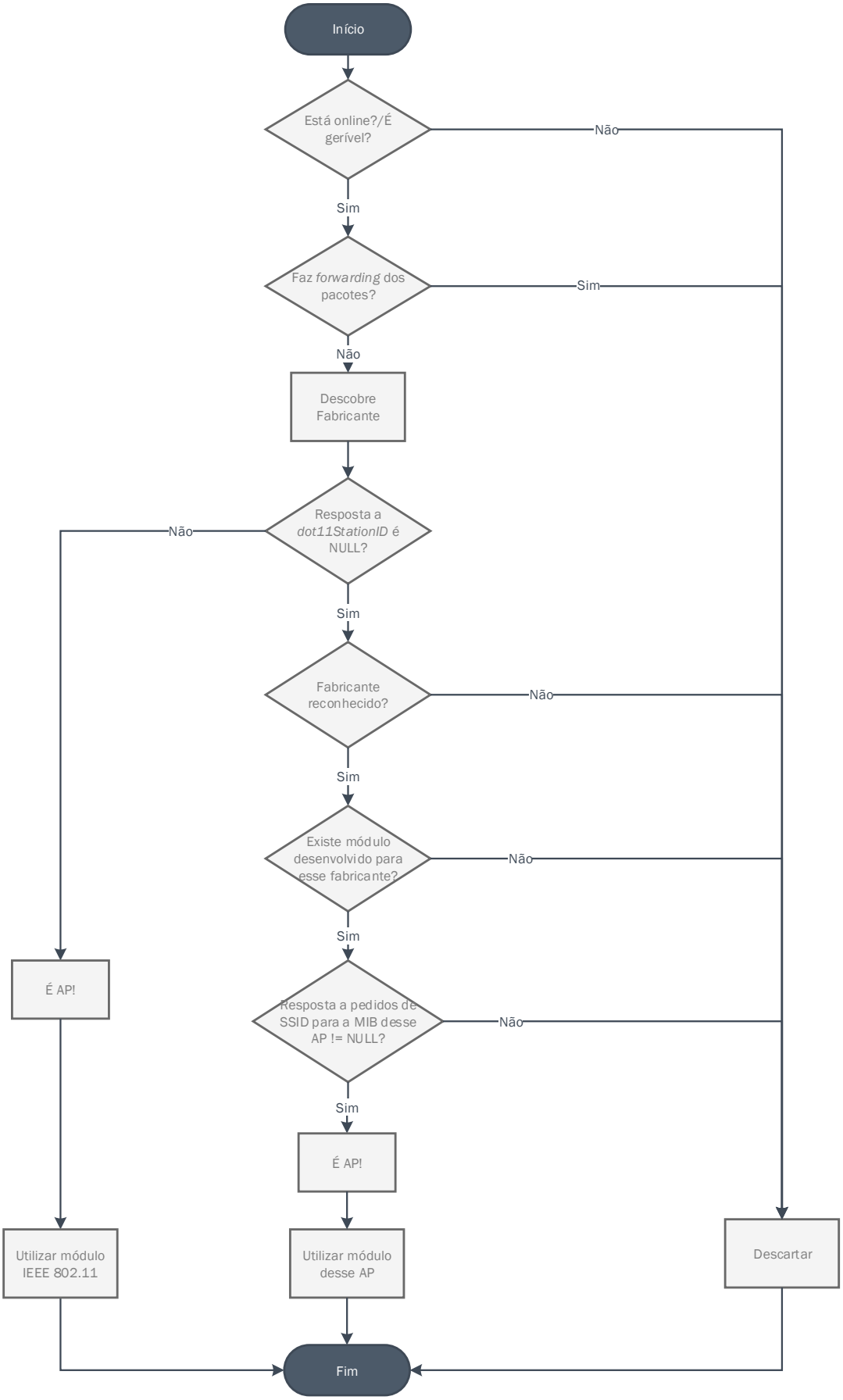


Figura 4.2: Pesquisa de rede.

4.2.2 Acesso às configurações dos APs

Um dos objetivos iniciais desta dissertação seria conseguir obter a maioria das informações dos APs, necessárias para a sua gestão, sem ser necessário recorrer às MIBs privadas dos fabricantes. Para isso, poderiam ser apenas utilizadas as informações provenientes das MIBs normalizadas (MIB-II e MIB IEEE802dot11). Teoricamente tal seria possível, mas na prática houve duas principais razões que tornaram essa ideia inviável: a maioria dos APs de teste utilizados neste projeto não ter a MIB IEEE802dot11 implementada e pelo facto dos APs mais antigos que contêm a MIB IEEE802dot11 implementada, não possuírem a versão de 2012, mas sim a de 2003. Por norma, estes equipamentos são os que funcionam apenas em modo autónomo. Esta diferença de versões, tal como já foi anteriormente referido no Capítulo 3, coloca entraves principalmente ao nível da gestão dos SSIDs e das estações associadas.

Para ultrapassar estas limitações, foi necessário recorrer às MIBs privadas. Assim, a recolha de informação do AP encontra-se dividida em quatro secções:

- **Informação geral do equipamento**: inclui o nome, os endereços MAC e IP, o canal utilizado para a transmissão de dados, o fabricante, o modelo, a versão do *firmware* e o endereço MAC da interface rádio. Este último parâmetro é importante sobretudo nos equipamentos que possuem duas interfaces rádio, como o AP Aruba;

- **Informação das interfaces**: como o índice, a descrição, o tipo e o estado de cada uma das interfaces, bem como o endereço IP do AP onde se insere a interface;

- **Informação sobre os SSIDs**: engloba informações desde o nome identificativo, se está ou não em *broadcast*, o BSSID, a VLAN, o endereço MAC do AP e se existe ou não segurança aplicada ao SSID;

- **Informações das estações**: incluindo o nome, os endereços MAC e IP, o modo de operação, o tipo, o SSID e os endereços MAC e IP do AP onde a estação se encontra associada.

Para a obtenção da informação necessária, foi preciso, em primeiro lugar, criar um método que inicie uma sessão para um agente SNMP remoto. Posto isto, foram desenvolvidos vários métodos para cada uma das secções. Estes métodos foram sub-divididos, por uma questão de organização, em módulos:

- módulo *infoSNMP*, comum a todos os APs onde é obtida informação mais geral do equipamento e onde é usada a MIB-II;

- módulo *IEEE802dot11*, dedicado a retirar informações dos APs que têm implementada a MIB IEEE802dot11, no caso dos APs em teste, destinado a retirar as informações dos dois APs da Cisco e do AP da TP-Link;

- módulo *Cisco*, utilizado para informações adicionais, específicas e não presentes na MIB IEEE802dot11, bem como para as informações sobre as estações associadas;

- módulo *DLink*, criado com o objetivo de obter informações sobre o AP do fabricante D-Link, bem como as respetivas estações ligadas;
- módulo *Aruba*, destinado a obter informações sobre o AP Aruba, bem como as respetivas estações ligadas.

Estes módulos foram desenvolvidos tendo em conta os equipamentos existentes para testes, mas caso seja necessário, facilmente se implementa e se adapta um novo conjunto de métodos para um fabricante diferente dos já existentes.

Seguidamente é feita a enumeração e descrição de cada um dos métodos criados, sendo descritos quais os seus objetivos e quais os módulos onde pertencem.

4.2.2.1 Informações gerais do equipamento

Nesta secção pretende-se obter o nome, a localização, o contacto, o endereço MAC, o canal, o modelo e a versão do *firmware* do equipamento. Para isso são usados os métodos descritos na tabela 4.3. É possível observar-se que, caso o AP contenha a MIB IEEE802dot11 não é necessário recorrer à sua MIB privada. Como nem todos os APs em teste contêm esta MIB implementada, são usados dois módulos de MIBs privadas: *Aruba* e *Dlink*.

4.2.2.2 Informação das interfaces

Na secção das interfaces é retirada informação detalhada sobre as interfaces do equipamento: qual o seu índice, a descrição, o tipo de interface e se se encontra *online*. Toda esta informação é obtida através da MIB-II sendo comum a qualquer equipamento.

4.2.2.3 Informação dos SSIDs

Pelo que se pode observar na tabela 4.5 existem quatro módulos diferentes de onde se pode retirar a informação necessária. Foi desenvolvido um módulo dedicado para as informações dos SSIDs dos APs Cisco porque, apesar de estes implementarem a MIB IEEE802dot11, não é possível obter informações relacionadas com diferentes SSIDs. Assim, todos os métodos preveem a possibilidade da existência de múltiplos SSIDs. A maneira como a MIB IEEE802dot11 está implementada no modelo da TP-Link, faz com que seja possível obter informações sobre os BSSID e sobre a presença de segurança.

Atributo	Módulo	Método	Descrição
Nome	infoSNMP	getsysName	Este método retorna uma *string* que contém o nome atribuído ao AP. Este parâmetro está contido na MIB-II, daí ser um atributo comum a todos os APs.
Localização	*infoSNMP*	getsysLocation	É retornada a *string* de localização do AP. Este atributo pode ser alterado pelo utilizador para fornecer informações úteis ou descrições sobre o local onde se encontra o equipamento. Trata-se de um objeto da MIB-II.
Contacto	*infoSNMP*	getsysContact	Retorna uma *string* que contém informação sobre o contacto do responsável pelo AP. Também este é um dos parâmetros disponibilizados pela MIB-II e que necessita de ser revisto pelo administrador.
Endereço MAC	*IEEE802dot11*	getMACAddress	Endereço MAC do equipamento em questão.
	Aruba	getMacAPAruba	
	Dlink	getMACdlink	
Canal	*IEEE802dot11*	getChannel	Informação sobre o canal onde está a ser feita a transmissão de dados.
	Aruba	getChannelAruba	
	Dlink	getChanneldlink	
Modelo	*IEEE802dot11*	getModel	Informação sobre o modelo do equipamento.
	Aruba	getModelAruba	Não é possível obter esta informação no AP D-Link.
Versão	*IEEE802dot11*	getVersion	Informação sobre a versão do equipamento.
	Aruba	getVersionAruba	
	Dlink	getVersiondlink	

Tabela 4.3: Informação geral do equipamento

4.2.2.4 Informação das estações

Todas as informações das estações são retiradas das MIBs privadas dos fabricantes. Como o AP da TP-Link não tem implementada a sua MIB privada, não é possível obter informações sobre as estações associadas a esse AP. Nem todas as MIBs contêm todos os detalhes sobre as estações conectadas, sendo que, no mínimo, todas contêm informações sobre o seu endereço MAC.

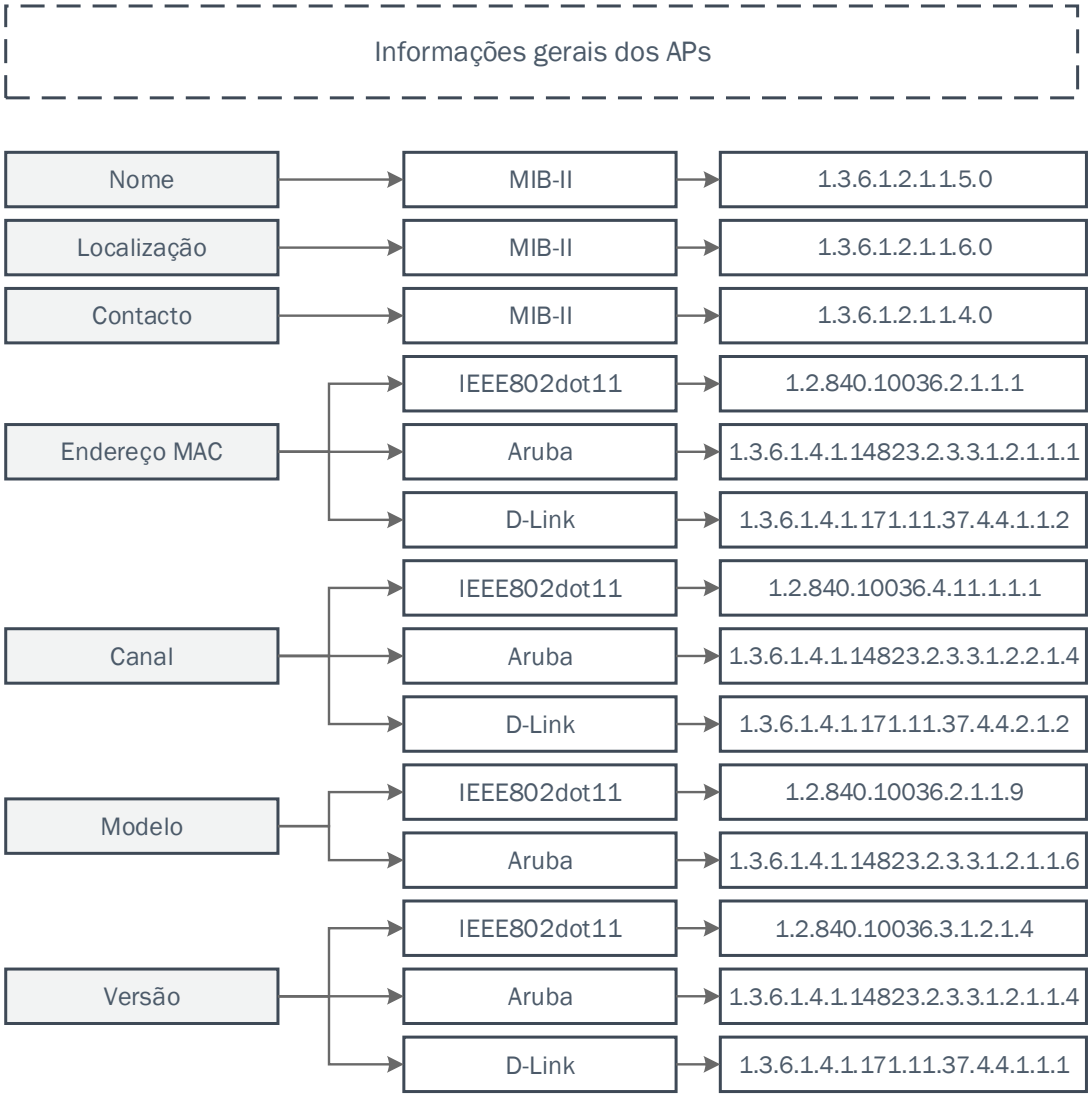


Figura 4.3: Informações gerais obtidas dos APs com a referência das respetivas MIBs e OIDs.

Atributo	Módulo	Método	Descrição
Índice	*infoSNMP*	getifIndex	Índice da interface correspondente ao objeto ifIndex. Este índice é único para cada interface do AP.
Descrição	*infoSNMP*	getifDescr	*String* que contém a descrição de cada uma das interfaces do AP.
Tipo	*infoSNMP*	getifType	Tipo atribuído à interface, sendo os tipos mais comuns no AP: other (1) ethernet (6) ieee802dot11(71) bridge (209)
Estado de Operação	*infoSNMP*	getifOperStatus	Estado de operação da interface, sendo os valores mais comuns: up (1) e down (2).

Tabela 4.4: Informação das interfaces

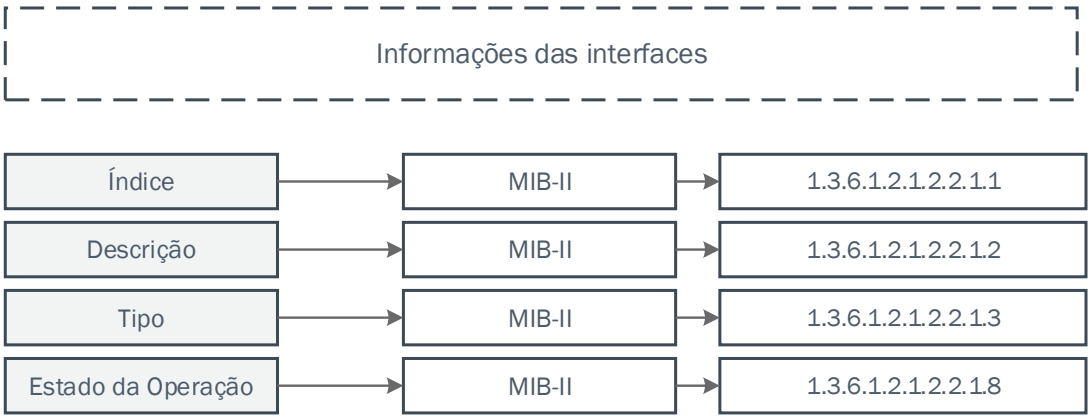


Figura 4.4: Informações sobre as interfaces dos APs, com a referência das respetivas MIBs e OIDs.

Atributo	Módulo	Método	Descrição
SSID	*Aruba*	getMultiSSIDAruba	SSIDs presentes no AP. Poderá ser retornado apenas um ou vários.
	Cisco	getCiscoMultiSSID	Não é possível obter esta informação do AP TP-Link, visto não se conseguir aceder à sua MIB privada.
	DLink	getSSIDdlink	
BSSID	*Aruba*	getMultiBSSIDAruba	BSSIDs correspondentes a cada SSID existente no AP.
	Cisco	getCiscoMultiBSSID	Não é possível obter esta informação do AP D-Link.
	IEEE802dot11	getBSSIDtplink	
VLAN	*Cisco*	getCiscoVlan	VLAN onde se encontra configurado o SSID.
	DLink	getVLANdlink	Esta informação não é possível ser retirada dos APs Aruba e TP-Link.
Segurança	*DLink*	getSecuritySSIDdlink	Este parâmetro serve apenas para indicar se existe algum tipo de segurança associada ao SSID ou não.
	IEEE802dot11	getSecSSIDtplink	Não é possível obter esta informação no AP Aruba nem nos APs da Cisco.
Broadcast	*Aruba*	getBroadcastSSID	Indica se o SSID está ou não em *broadcast*, tendo também em consideração se a interface rádio se encontra ligada ou desligada.
	Cisco	getBroadcastSSIDCisco	Não existe nenhum parâmetro dedicado a esta informação no AP TP-Link, mas caso o SSID não se encontre em *broadcast* e devido à má implementação da MIB IEEE802dot11 neste equipamento, também não é possível obter qualquer informação contida nessa MIB.
	DLink	getBroadcastSSIDdlink	

Tabela 4.5: Informação acerca dos SSIDs

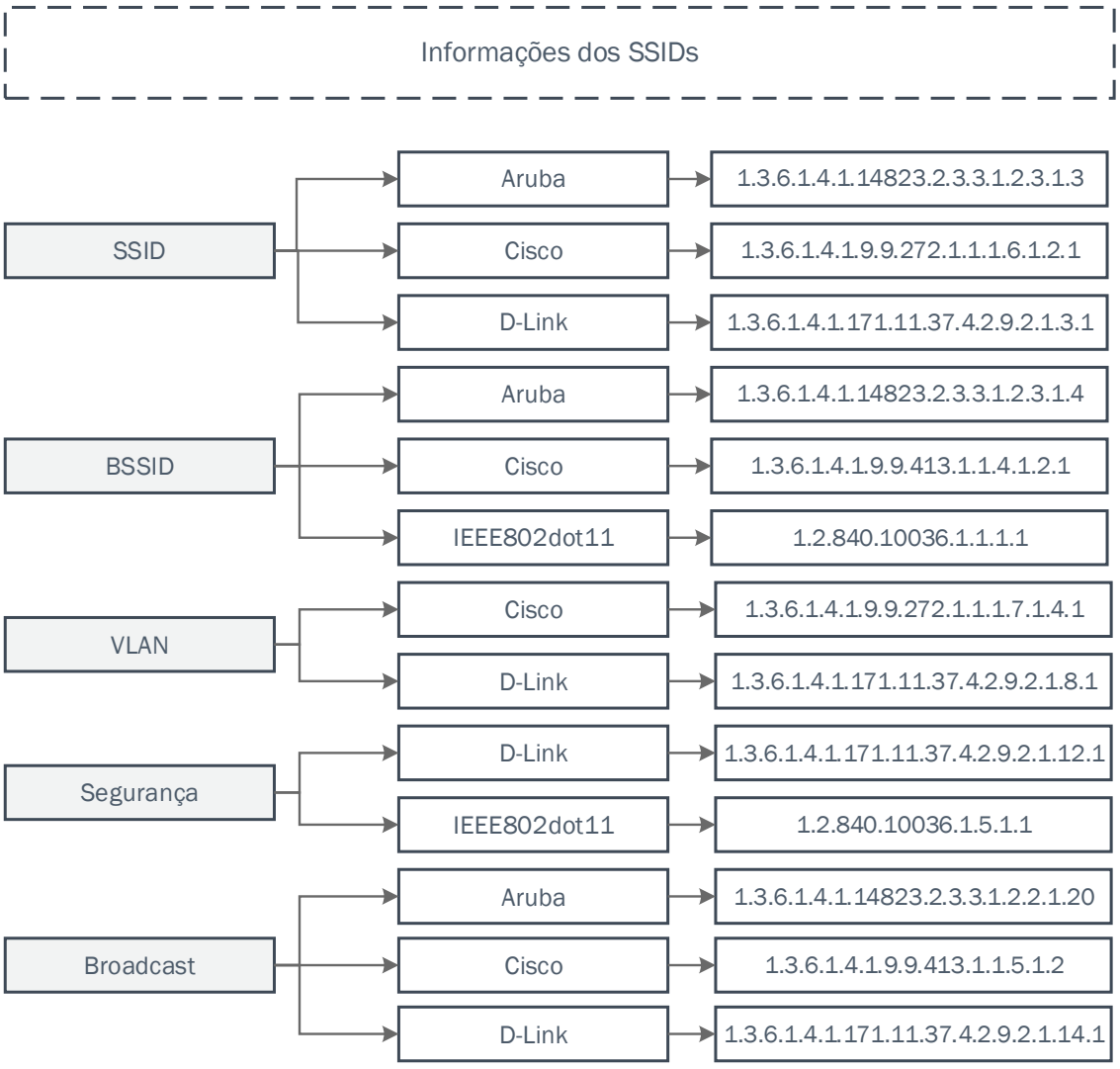


Figura 4.5: Informações sobre os SSIDs existentes, com a referência das respetivas MIBs e OIDs.

Atributo	Módulo	Método	Descrição
Nome	*Aruba*	getNameDevicesAruba	Nome atribuído a cada uma das estações.
	Cisco	getNameDevices	
Endereço IP	*Aruba*	getIPDevicesAruba	Endereço IP de cada uma das estações.
	Cisco	getIP	
Endereço MAC	*Aruba*	getMACAddDevicesAruba	Endereço MAC de cada uma das estações.
	Cisco	getMAC	
	Dlink	getMacAddressSTAdlink	
SSID	*Aruba*	getDevSSIDAruba	SSID onde as estações se encontram conectadas.
	Cisco	getSSID	
	Dlink	getSSIDdlinkSTA	
Modo	*Cisco*	getMode	Nos APs da Cisco, é retornado o *standard* do IEEE 802.11 que se aplica à interface radio da estação, podendo conter valores como: ieee802dot11a (1) - *standard* IEEE802.11a ieee802dot11b (2) - *standard* IEEE802.11b ieee802dot11g (3) - *standard* IEEE802.11g
	Dlink	getTypedlink	Nos APs da D-Link é retornada também a banda do cliente podendo tomar os valores: 0 - *standard* IEEE 802.11a 1 - *standard* IEEE 802.11b 2 - *standard* IEEE 802.11g
Tipo	*Cisco*	getType	Indica o tipo de cliente. Salientam-se os seguintes valores: unkown (1) generic80211Client (104)

Tabela 4.6: Informação das estações

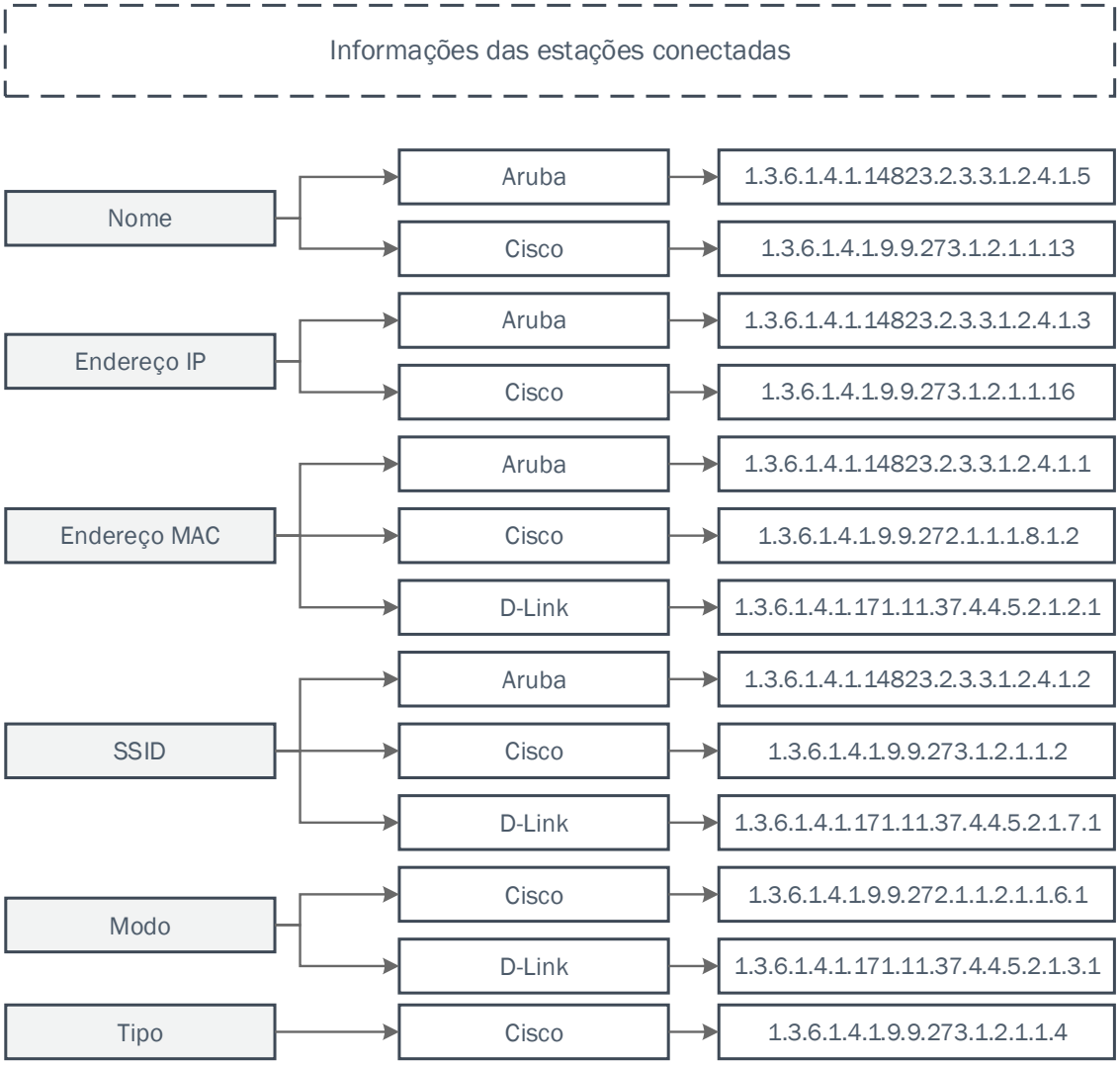


Figura 4.6: Informações sobre as estações conectadas aos APs existentes, com a referência das respetivas MIBs e OIDs.

4.2.3 Alteração das configurações dos APs

A alteração das configurações dos APs é limitada à permissão existente para os objetos das MIBs. Há certos parâmetros, como os endereços MAC, as informações sobre as interfaces ou sobre as estações associadas, que não podem ser alteradas de modo algum.

À semelhança do que acontece no acesso às configurações dos APs, também na alteração das configurações o projeto está organizado em secções:

- Alteração das informações gerais do equipamento como o nome, o contacto, a localização, o canal e o endereço IP;
- Modificação dos SSIDs e informações associadas, como o nome identificativo da rede, a permissão de *broadcast* e as VLANs.

Seguindo o processo anterior de leitura, também na escrita dos APs, as secções foram subdivididas em módulos:

- módulo *infoSNMP*, comum a todos os APs onde se pode alterar informação mais geral do equipamento;
- módulo *Cisco*, utilizando as MIBs do fabricante Cisco para alterar certos parâmetros;
- módulo *Dlink*, criado com o objetivo de alterar parâmetros utilizando a MIB privada da D-Link.

4.2.3.1 Informações gerais do equipamento

Tal como já foi referido, nem todas as informações poderão ser alteradas por não terem permissão *read-write*. Neste caso, apenas com o AP da D-Link é possível alterar o canal, visto não existirem permissões na MIB privada da Cisco e não ser também possível fazer alteração desse parâmetro através da MIB IEEE802dot11, devido a problemas de implementação.

Atributo	Módulo	Método	Descrição
Nome	*infoSNMP*	SetSysName	Alteração do nome do AP conforme informação enviada pelo utilizador.
Contacto	*infoSNMP*	SetSysContact	Alteração do contacto do administrador do AP conforme informação enviada pelo utilizador.
Localização	*infoSNMP*	SetSysLocation	Alteração da descrição da localização do AP conforme informação enviada pelo utilizador.
Canal	*Dlink*	SetChannel	Alteração do canal do AP. Apenas é possível fazer esta alteração no AP da D-Link.
Endereço IP	*Dlink*	SetIP	Alteração do endereço IP do AP. Apenas é possível fazer esta alteração no AP da D-Link.

Tabela 4.7: Alteração das configurações gerais do AP

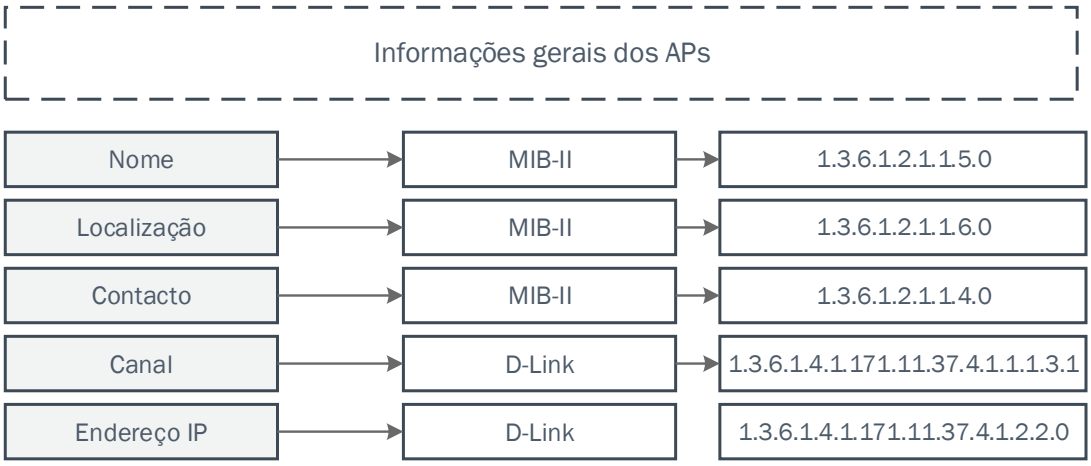


Figura 4.7: Parâmetros relativos ao AP que podem ser alterados, com a referência das respetivas MIBs e OIDs.

4.2.3.2 Informações dos SSIDs

As informações dos SSIDs poderão ser alteradas conforme pedido do utilizador. Poderá ser alterado o SSID, o *broadcast* apenas no caso do AP-Dlink e a VLAN onde se inserem.

Atributo	Módulo	Método	Descrição
SSID	Cisco	SetSSID_user	Alteração dos SSIDs existentes, consoante informação enviada pelo utilizador.
	Dlink	SetSSID_user	
Broadcast	Dlink	SetBroadSSID	Alteração do estado do *broadcast*, consoante informação enviada pelo utilizador.
VLAN	Cisco	SetVlan	Alteração das VLANs existentes, consoante informação enviada pelo utilizador.
	Dlink	SetVlan	

Tabela 4.8: Alteração das configurações dos SSIDs

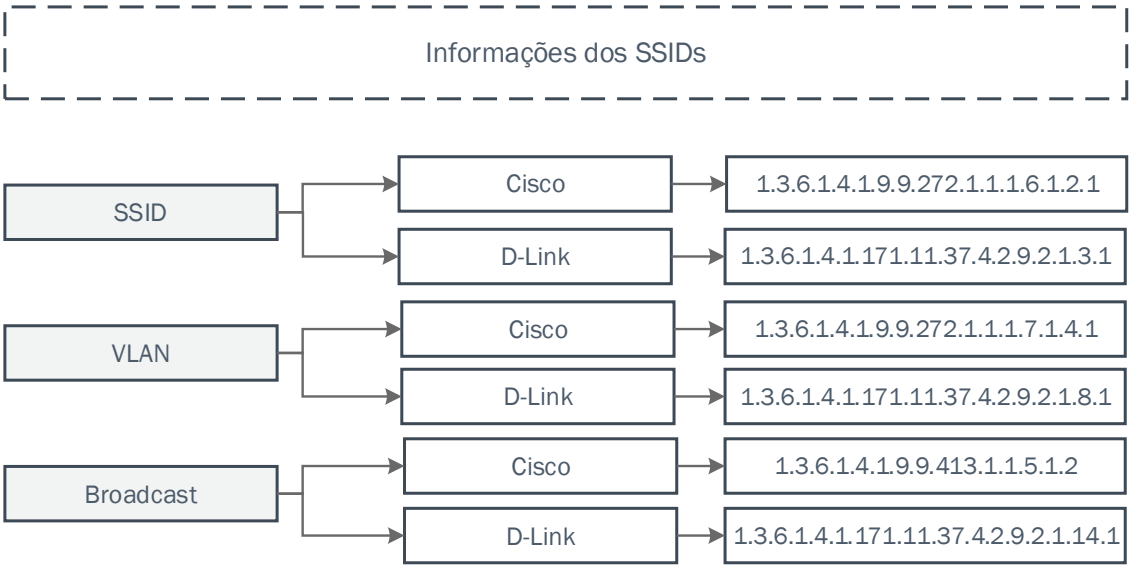


Figura 4.8: Parâmetros relativos aos SSIDs que podem ser alterados, com a referência das respetivas MIBs e OIDs.

4.2.4 Base de dados

A base de dados, tal como já foi referido, é MySQL e faz a ligação entre o *back-end* e o *front-end*, guardando toda a informação gerada durante as diferentes iterações.

Assim, esta base de dados é constituída por cinco tabelas: *Info_AP*, *interface*, *SSID_info*, *Info_STA* e *Network*.

Todas as entradas nas tabelas são compostas por um número identificativo e único dentro dessa tabela, atribuído e incrementado sempre que são adicionadas novas informações. A cada entrada é também adicionado um *timestamp*.

Na tabela *Info_AP* são guardadas todas as informações gerais do AP, correspondentes à secção da informação geral do equipamento no acesso aos APs, quer o objetivo do acesso seja a leitura ou a escrita de objetos, como os endereços IP, MAC e o endereço MAC da interface rádio do equipamento. Este último poderá ser diferente do endereço MAC nos APs que contêm duas interfaces rádio, como é o caso do AP Aruba. Também o nome, a localização, o contacto, o fabricante, o modelo, a versão do *firmware* e o canal de transmissão são objetos guardados nesta tabela, bem como o resultado da pesquisa do objeto *ipForwarding* da MIB-II e o parâmetro *ReadWrite* que apresenta a indicação se o pedido feito pelo utilizador foi de leitura (0) ou de escrita (1). Quando o utilizador tem como objetivo a alteração das configurações dos APs há dois campos desta tabela que também deverão ser preenchidos a *community* para que a escrita seja possível e, se for caso disso, o endereço IP que se quer alterar.

Na tabela *interface* apenas são guardadas as informações obtidas sobre as interfaces, visto não ser possível alterar a sua informação. É inserida uma entrada nova na tabela por cada interface, contendo o respetivo índice, a descrição, o tipo, o estado e o endereço IP do equipamento ao qual a interface pertence.

A tabela *SSID_info* é usada para guardar informação relativa aos SSIDs: o nome da rede, o BSSID, a VLAN, o estado da segurança e do *broadcast*, bem como os endereços MAC e IP do equipamento. À semelhança da tabela que guarda a informação geral dos APs, também esta contém o parâmetro *ReadWrite*, devido à possibilidade de se poder alterar as configurações dos SSIDs. São também armazenadas informações de outros objetos como a identificação do fabricante, para se fazer a diferenciação na execução dos métodos de escrita para cada um dos APs, e a *community*.

As informações das estações conectadas a cada AP estão presentes na tabela *Info_STA*, contendo o nome da estação, os seus endereços MAC e IP, o SSID onde se encontra conectada, bem como o modo de operação, o tipo de estação e o endereço IP do AP.

A tabela *Network* existe para guardar os parâmetros inseridos pelo utilizador quando é requerida uma pesquisa. Guarda os valores de início e de fim de uma gama de IPs ou a rede no formato *rede/máscara*, dependendo do método escolhido pelo utilizador para efetuar a sua pesquisa. Também a *community* para autorizar a recolha de informação através do protocolo SNMP é inserida nesta tabela. O parâmetro *FLAG_lock* é fundamental para existir sincronização entre a leitura e a escrita: se algum dos processos estiver a decorrer, é atribuído a este campo o valor 1, não sendo,

então, possível adicionar qualquer tipo de informação à base de dados. Este parâmetro volta a ter o valor 0 quando o processo termina.

Tal como se pode verificar nas imagens 4.9 e 4.10, se o utilizador pretender fazer a pesquisa de uma rede ou de uma gama de endereços IP, insere esses parâmetros na interface *web*. Essa informação será guardada de seguida na tabela *Network*, onde a *FLAG_lock* é colocada a 1. Caso o utilizador deseje alterar as configurações do AP ou dos SSIDs, as informações são inseridas na tabela *Info_AP* ou *SSID_info*, respetivamente e, para além da ativação da *FLAG_lock*, é também inserido o valor 1 no parâmetro *ReadWrite*.

O *back-end*, durante a verificação periódica dos valores da base de dados, feita através de um *cronjob*, recolhe os dados da tabela *Network* e os dados do parâmetro *ReadWrite* mais recentes. Esses dados são, então, reencaminhados para os módulos de acesso ao AP. No fim da pesquisa ou da alteração de configurações, os valores atualizados são inseridos em cada uma das tabelas da base de dados.

A interface *web* apresenta sempre os dados mais recentes. Para isso, e como há várias entradas da mesma ordem de pesquisa em cada uma das tabelas com valores semelhantes, mas diferindo de alguns segundos, foi desenvolvido um método que permite agrupar as entradas das tabelas: a construção de um intervalo de tempo, com um limite superior de mais quatro segundos e um limite inferior de menos quatro segundos relativamente ao valor mais recente do *timestamp*. Assim, todas as entradas com um *timestamp* dentro desses limites podem ser consideradas como as mais recentes.

4.2.4.1 Sincronização

Para que a monitorização da rede seja feita de uma maneira eficiente e periódica, recorreu-se à utilização de um *cronjob* que executa um *script* de minuto a minuto.

Nesse ficheiro é verificado, em primeiro lugar, se já passaram 5 minutos desde as últimas alterações na tabela *Network*. Caso se verifique essa condição e caso tenha ocorrido um erro, ou seja, caso a *FLAG_lock* se mantenha a 1, esta é desativada para que o utilizador possa fazer uma nova pesquisa.

É também examinada a possibilidade de existir alguma alteração nos últimos 40 segundos. Caso seja verdade e a *flag* se encontre a 0, é ativada e é verificado o pedido do utilizador: se se trata de uma alteração de configuração de SSIDs, de APs ou de uma pesquisa. Essa informação é depois reencaminhada para os módulos de acesso aos APs.

Se esta última condição não se verificar e se já tiverem decorrido mais de dois minutos desde a última pesquisa ou alteração na rede, é feita uma nova pesquisa automática para que a informação sobre os APs esteja sempre o mais atualizada possível.

Os valores do tempo foram atribuídos empiricamente e de acordo com os testes realizados com o material disponível, podendo ser posteriormente adaptados, se assim for necessário, a diferentes redes.

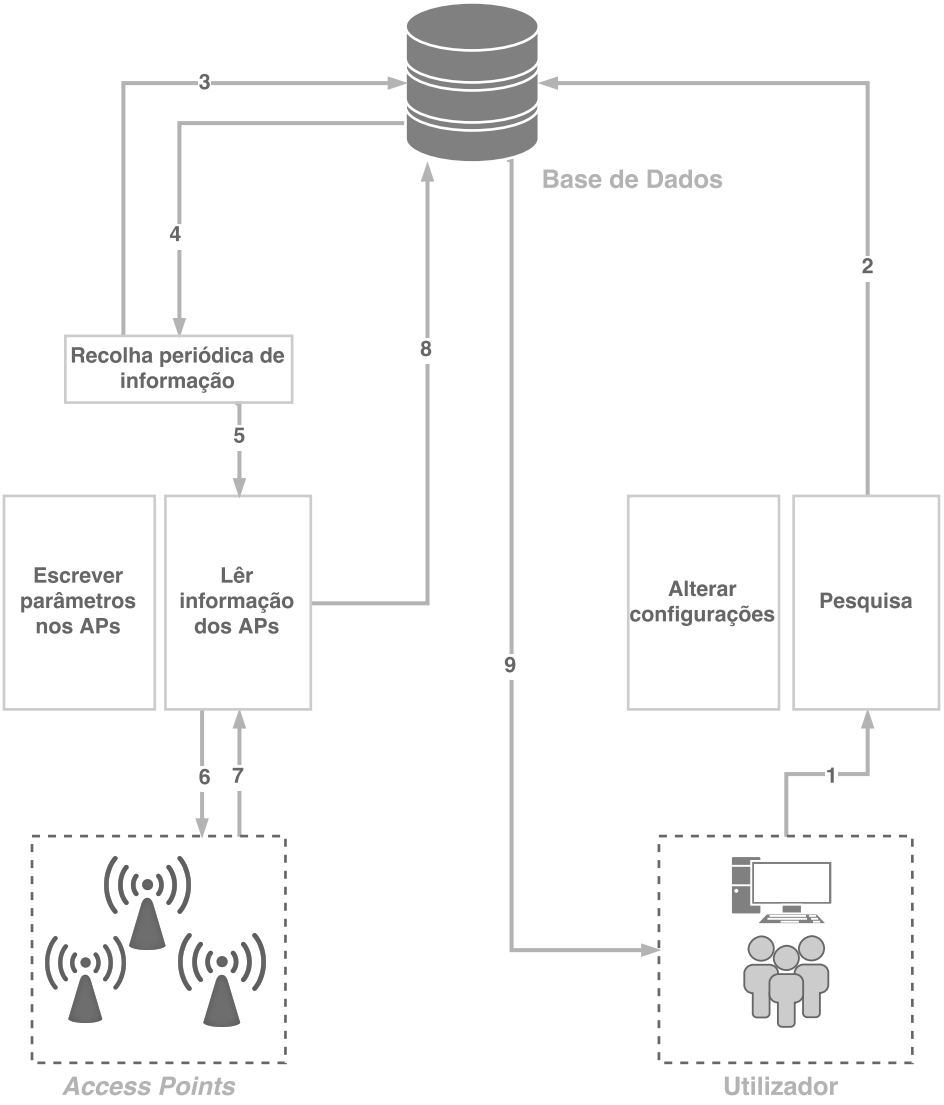


Figura 4.9: Fluxo de dados caso seja requerido pelo utilizador uma pesquisa da rede.

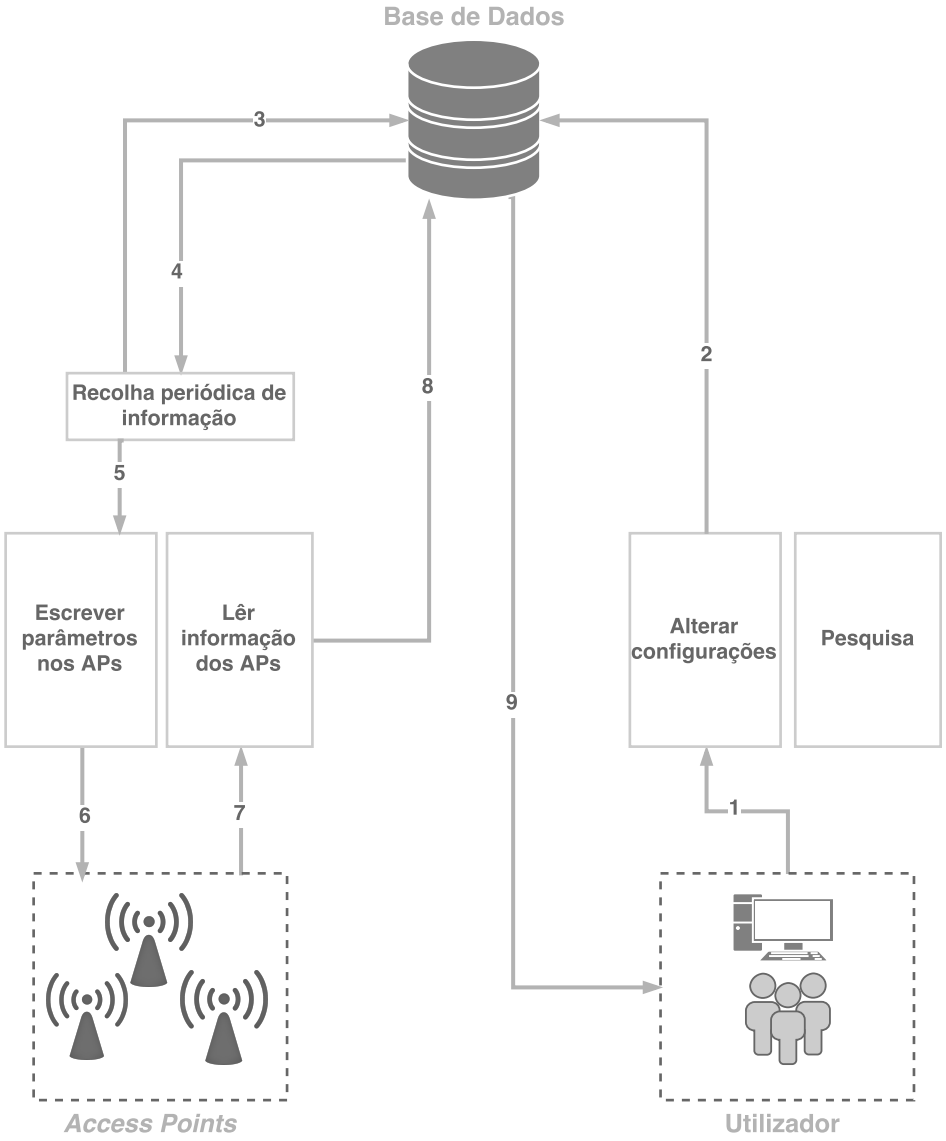


Figura 4.10: Fluxo de dados caso seja requerido pelo utilizador uma alteração das configurações dos APs.

4.2.5 Interface gráfica

A interface gráfica pertence ao *front-end* e tem como objetivo colecionar os dados presentes na base de dados e apresentá-los ao utilizador. Esta interface foi desenvolvida a partir de um servidor *web* e pode ser consultada como um *website* normal, a partir de um *browser*.

Para o desenvolvimento gráfico foi utilizada uma *framework* - o Bootstrap, visto ser uma ferramenta bastante completa.

A interface *web* é dividida em cinco menus diferentes que irão ser descritos de seguida.

4.2.5.1 Início

Esta é a secção inicial do projeto.

Figura 4.11: Interface Gráfica: Secção Inicial.

4.2.5.2 Pesquisa

Esta é a secção onde o utilizador pode inserir os dados da rede ou da gama de IPs que pretende pesquisar.

São necessários os seguintes dados:

- **Rede**: no formato IP/máscara, no caso de se pretender fazer a pesquisa de uma rede completa;
- **Endereço de Início**: no caso de se pretender fazer a pesquisa de uma gama de IPs este é o endereço do início da gama endereços a pesquisar;
- **Endereço de Fim**: no caso de se pretender fazer a pesquisa de uma gama de IPs este é o endereço do fim da gama de endereços a pesquisar;
- ***Community* de leitura**: obrigatória para qualquer um dos métodos de pesquisa, para que seja possível aceder aos objetos dos APs através do protocolo SNMP.

Caso se pretenda fazer a pesquisa de uma rede completa (IP/máscara) não se deverá preencher os campos de endereço de início e endereço de fim, bem como se se pretender pesquisar uma gama de endereços IPs também não se deverá preencher o campo Rede. Tal como se pode verificar na Figura 4.12, existe um aviso para esclarecer o utilizador de como efectuar a pesquisa corretamente. Caso o campo a vermelho esteja ativo, qualquer pesquisa inserida durante esse período não será validada.

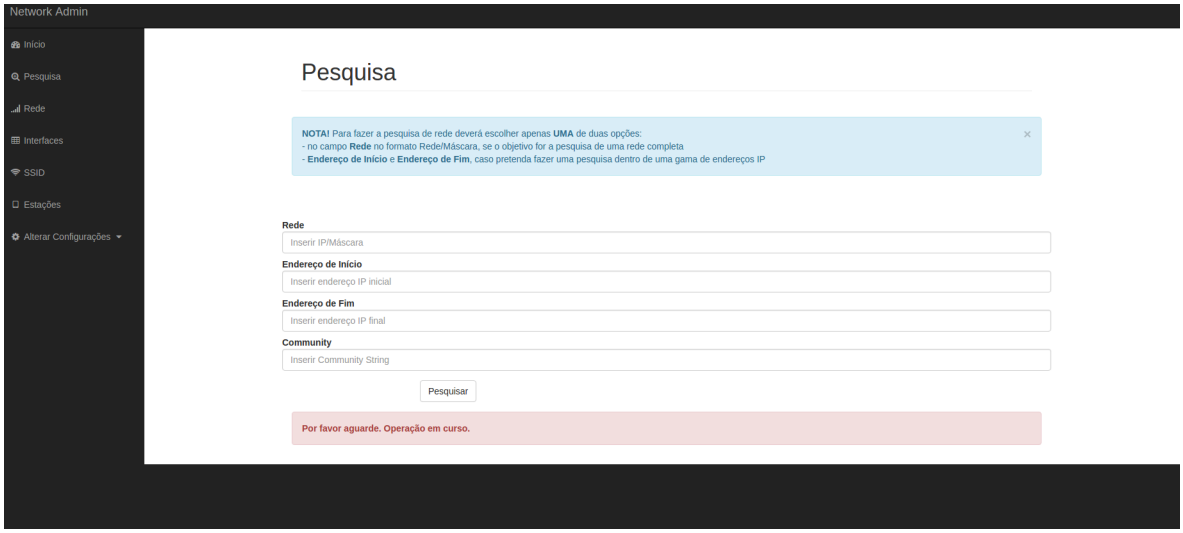


Figura 4.12: Interface Gráfica: Secção de Pesquisa.

4.2.5.3 Rede

No menu Rede é possível visualizar todas as informações gerais do AP, bem como um grafo que contém a rede, os APs monitorizados dessa rede e as estações ligadas a esses APs.

Na tabela Rede é possível observar o número único identificativo do AP, o seu endereço IP, o seu nome, contacto e localização. Também se encontram presentes o endereço MAC da interface rádio, o canal de transmissão, o fabricante, o modelo, a versão do *firmware* e o *timestamp* que indica a data e a hora a que foi recolhida informação.

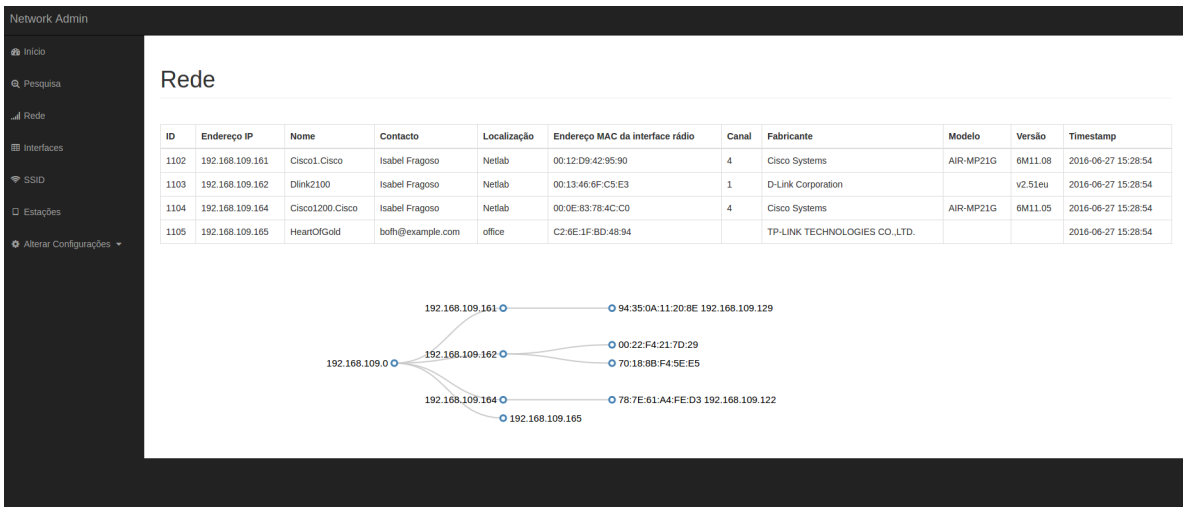


Figura 4.13: Interface Gráfica: Secção da Rede.

4.2.5.4 Interfaces

Sobre as interfaces é possível observar as informações sobre o índice, a descrição da interface, o tipo e o estado de cada uma das interfaces, bem como, o endereço IP do AP a que pertence. Encontra-se também o *timestamp* que indica a data e a hora a que foi recolhida informação.

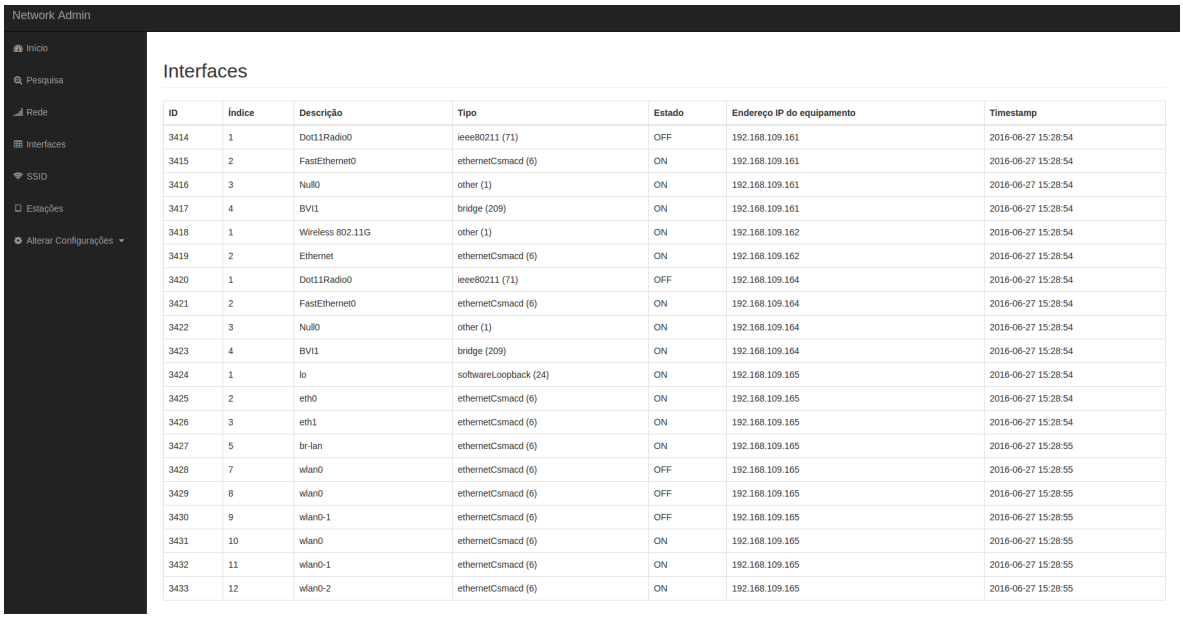
4.2.5.5 SSID

Nesta secção é possível encontrar toda a informação acerca dos SSIDs, como a identificação única do SSID, o estado do *broadcast*, o BSSID, a VLAN, o estado da implementação de autenticação, o endereço MAC do AP onde o SSID está inserido e o *timestamp* que indica a data e a hora a que foi recolhida informação.

4.2.5.6 Estações

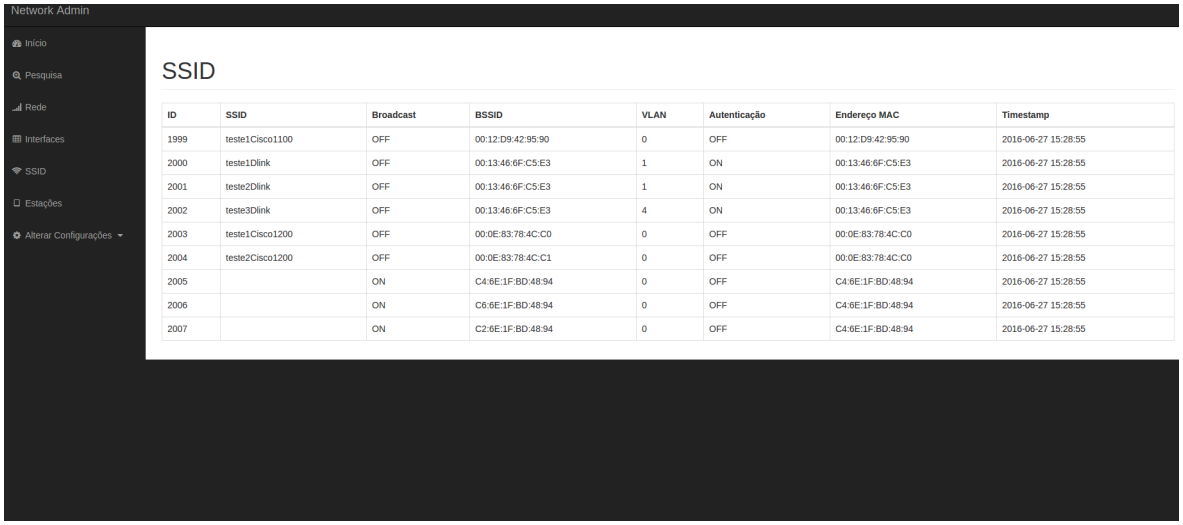
Nesta secção é possível encontrar toda a informação acerca das estações.

Aqui é possível obter informações sobre a identificação da estação, o nome, os endereços MAC e IP, o SSID onde a estação se encontra conectada, bem como os endereços MAC e IP do



ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento	Timestamp
3414	1	Dot11Radio0	ieee80211 (71)	OFF	192.168.109.161	2016-06-27 15:28:54
3415	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.161	2016-06-27 15:28:54
3416	3	Null0	other (1)	ON	192.168.109.161	2016-06-27 15:28:54
3417	4	BVI1	bridge (209)	ON	192.168.109.161	2016-06-27 15:28:54
3418	1	Wireless 802.11G	other (1)	ON	192.168.109.162	2016-06-27 15:28:54
3419	2	Ethernet	ethernetCsmacd (6)	ON	192.168.109.162	2016-06-27 15:28:54
3420	1	Dot11Radio0	ieee80211 (71)	OFF	192.168.109.164	2016-06-27 15:28:54
3421	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.164	2016-06-27 15:28:54
3422	3	Null0	other (1)	ON	192.168.109.164	2016-06-27 15:28:54
3423	4	BVI1	bridge (209)	ON	192.168.109.164	2016-06-27 15:28:54
3424	1	lo	softwareLoopback (24)	ON	192.168.109.165	2016-06-27 15:28:54
3425	2	eth0	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:54
3426	3	eth1	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:54
3427	5	br-lan	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:55
3428	7	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 15:28:55
3429	8	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 15:28:55
3430	9	wlan0-1	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 15:28:55
3431	10	wlan0	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:55
3432	11	wlan0-1	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:55
3433	12	wlan0-2	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 15:28:55

Figura 4.14: Interface Gráfica: Secção das interfaces.



ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC	Timestamp
1999	teste1Cisco1100	OFF	00:12:D9:42:95:90	0	OFF	00:12:D9:42:95:90	2016-06-27 15:28:55
2000	teste1Dlink	OFF	00:13:46:6F:C5:E3	1	ON	00:13:46:6F:C5:E3	2016-06-27 15:28:55
2001	teste2Dlink	OFF	00:13:46:6F:C5:E3	1	ON	00:13:46:6F:C5:E3	2016-06-27 15:28:55
2002	teste3Dlink	OFF	00:13:46:6F:C5:E3	4	ON	00:13:46:6F:C5:E3	2016-06-27 15:28:55
2003	teste1Cisco1200	OFF	00:0E:83:78:4C:C0	0	OFF	00:0E:83:78:4C:C0	2016-06-27 15:28:55
2004	teste2Cisco1200	OFF	00:0E:83:78:4C:C1	0	OFF	00:0E:83:78:4C:C0	2016-06-27 15:28:55
2005		ON	C4:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 15:28:55
2006		ON	C6:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 15:28:55
2007		ON	C2:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 15:28:55

Figura 4.15: Interface Gráfica: Secção dos SSID.

AP. Também o modo e o tipo da estação bem como o *timestamp* que indica a data e a hora a que foi recolhida informação, se encontram representados nesta tabela.

4.2.5.7 Alteração de Configurações

Esta é a secção onde é possível alterar as configurações dos APs. Assim, pelo menu *dropdown*, é possível escolher a opção de alterar as configurações gerais do AP ou os SSIDs.

Para alterar as configurações gerais do AP basta indicar o ID do AP onde se quer alterar as configurações e escrever nos campos que se pretendem alterar. É necessário ter em atenção que

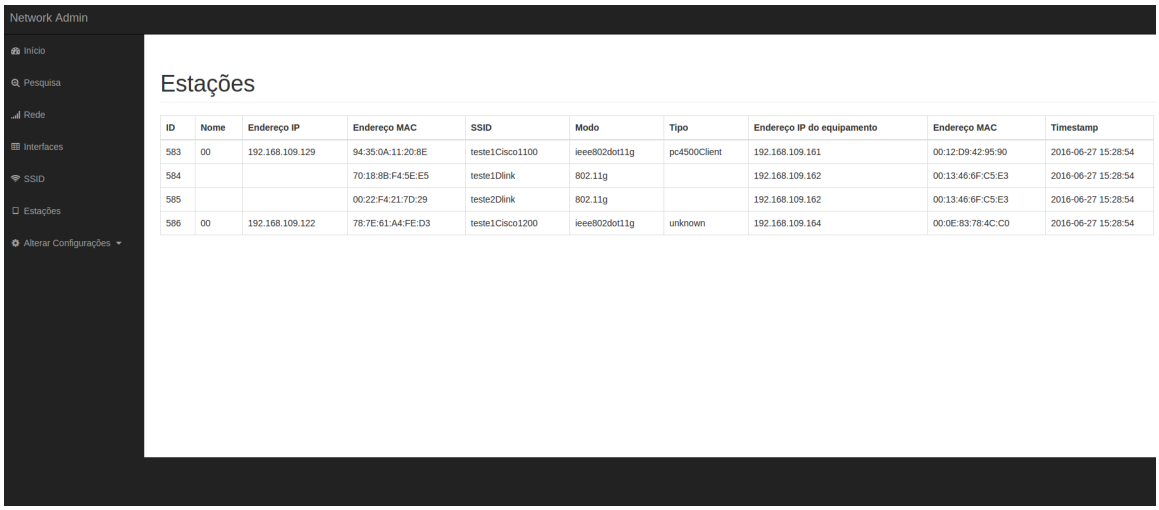


Figura 4.16: Interface Gráfica: Secção das Estações.

o canal e o endereço IP apenas poderão ser alterados em APs do fabricante D-Link. Por fim, é necessário indicar a *Community* para a escrita dos APs.

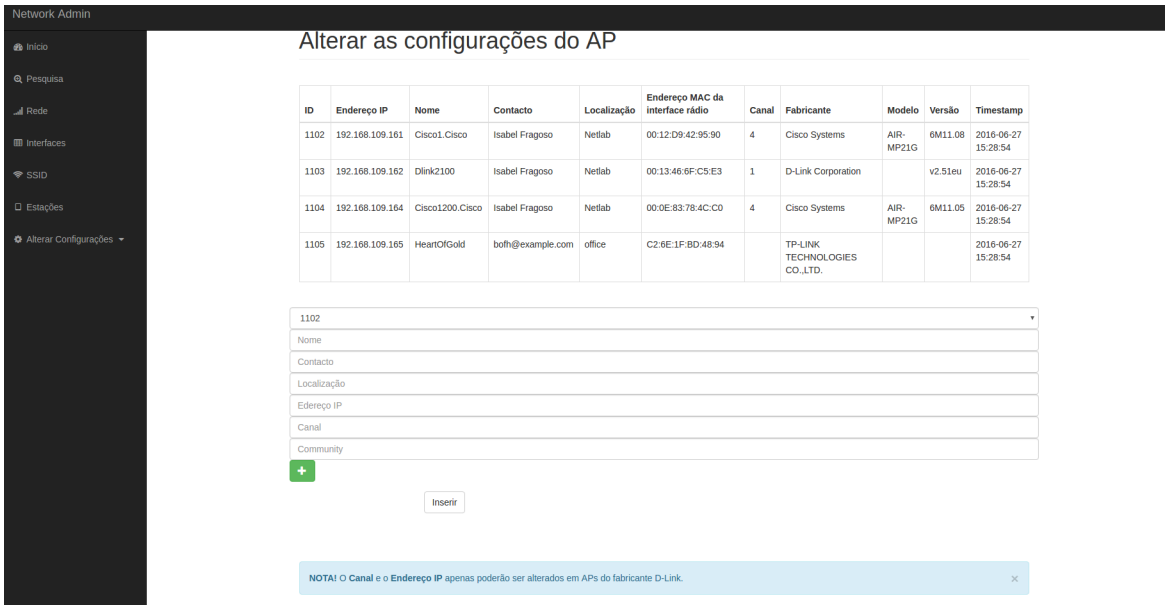


Figura 4.17: Interface Gráfica: Secção da alteração de configurações do AP.

No caso de se querer alterar as configurações dos SSIDs é necessário identificar o SSID através do seu número único presente no menu *dropwdown* e escrever nos campos onde se pretender alterar a informação. O parâmtro *Broadcast* apenas poderá ser alterado nos APs do fabricante D-Link. Se se pretender que este seja ativo é necessário ligar a interface rádio do equipamento. A *Community* de escrita é absolutamente necessária para se poderem fazer as alterações pretendidas.

Tanto na página de alteração das configurações dos APs como nos SSIDs, poder-se-á fazer

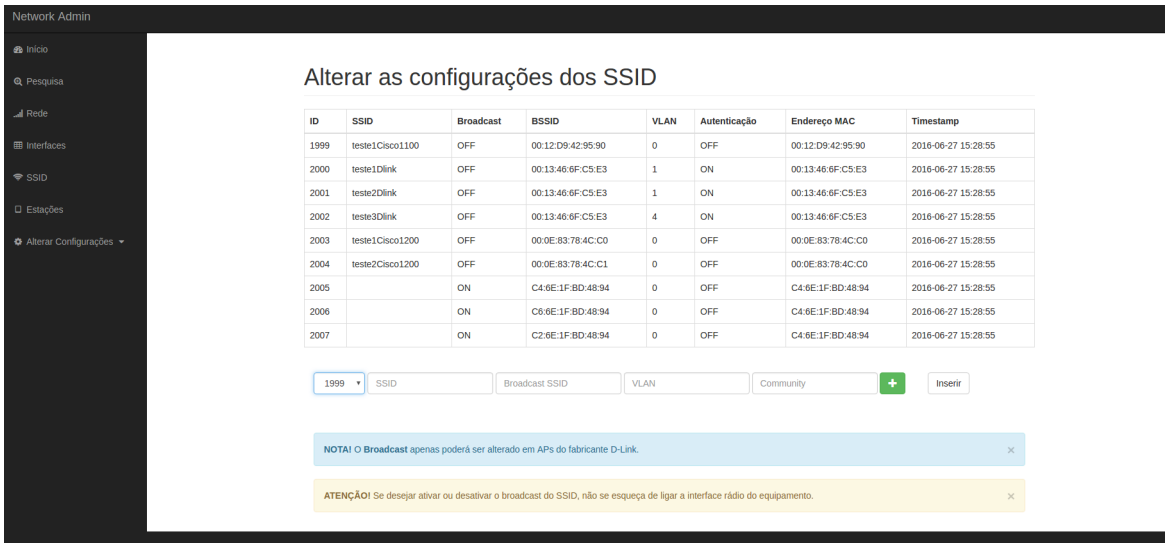


Figura 4.18: Interface Gráfica: Secção da alteração de configurações dos SSIDs.

modificações em mais do que um AP na mesma iteração. Para isso basta carregar no botão verde com o sinal "+". Não será possível existirem dois conjuntos de alterações com o mesmo número de identificação.

4.3 Validação da solução

Nesta secção é feita a demonstração do bom funcionamento da ferramenta desenvolvida.

4.3.1 APs utilizados para testes

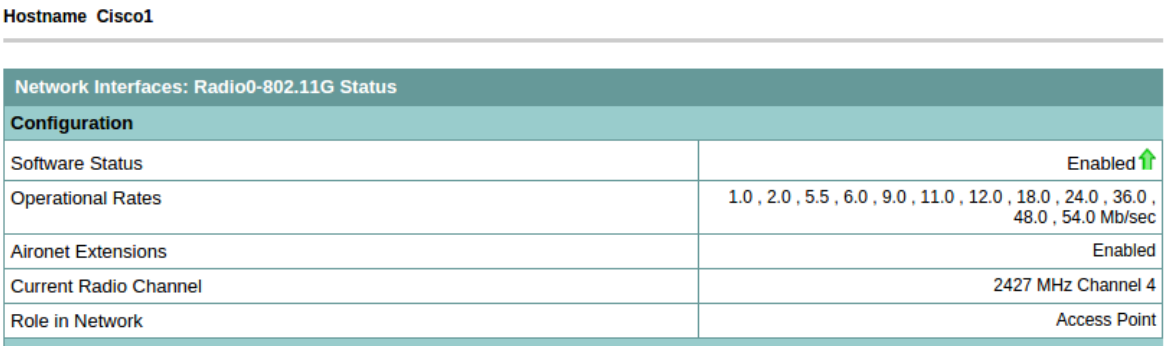
Para a validação da solução foram retiradas algumas imagens das interfaces gráficas originais dos APs e do projeto desenvolvido, para se poder comparar a veracidade das informações.

Devido à grande quantidade de imagens existentes, apenas serão aqui expostas as informações do AP Cisco 1100, sendo que as provas dos restantes APs de teste se encontram no anexo A.

Hostname Cisco

Home: Summary Status		
Association		
Clients: 0		Infrastructure clients: 0
Network Identity		
IP Address		192.168.109.161
MAC Address		0012.0026.9e6a
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0012.0026.9e6a	100Mb/s
Radio0-802.11G	0012.d942.9590	54.0Mb/s

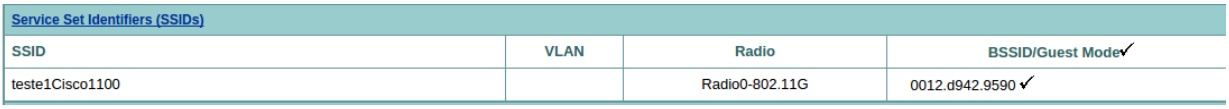
(a) Informação geral.



Hostname Cisco1

Network Interfaces: Radio0-802.11G Status	
Configuration	
Software Status	Enabled
Operational Rates	1.0 , 2.0 , 5.5 , 6.0 , 9.0 , 11.0 , 12.0 , 18.0 , 24.0 , 36.0 , 48.0 , 54.0 Mb/sec
Aironet Extensions	Enabled
Current Radio Channel	2427 MHz Channel 4
Role in Network	Access Point

(b) Interface Rádio.



Service Set Identifiers (SSIDs)			
SSID	VLAN	Radio	BSSID/Guest Mode
teste1Cisco1100		Radio0-802.11G	0012.d942.9590 ✓

(c) SSIDs.

Figura 4.19: Informação sobre o AP Cisco 1100 retirada da interface gráfica do equipamento.

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão
1133	192.168.109.161	Cisco1.Cisco	Isabel Fragoso	Netlab	00:12:D9:42:95:90	4	Cisco Systems	AIR-MP21G	6M11.08

(a) Informação geral.

Interfaces

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento
3588	1	Dot11Radio0	ieee80211 (71)	ON	192.168.109.161
3589	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.161
3590	3	Null0	other (1)	ON	192.168.109.161
3591	4	BVI1	bridge (209)	ON	192.168.109.161

(b) Interfaces.

SSID

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC
2065	teste1Cisco1100	ON	00:12:D9:42:95:90	0	OFF	00:12:D9:42:95:90

(c) SSIDs.

Figura 4.20: Informação sobre o AP Cisco 1100 retirada da ferramenta desenvolvida.

4.3.2 Cenário de teste - rede no laboratório

Uma das redes utilizadas para teste é composta por quatro APs. Depois de uma pesquisa à rede 192.168.109.0/24 foi possível obterem-se as seguintes informações através da ferramenta desenvolvida.

Rede

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão	Timestamp
1129	192.168.109.161	Cisco1.Cisco	Isabel Fragoso	Netlab	00:12:D9:42:95:90	4	Cisco Systems	AIR-MP21G	6M11.08	2016-06-27 17:33:20
1130	192.168.109.162	Dlink2100	Isabel Fragoso	Netlab	00:13:46:6F:C5:E3	1	D-Link Corporation		v2.51eu	2016-06-27 17:33:22
1131	192.168.109.164	Cisco1200.Cisco	Isabel Fragoso	Netlab	00:0E:83:78:4C:C0	4	Cisco Systems	AIR-MP21G	6M11.05	2016-06-27 17:33:23
1132	192.168.109.165	HeartOfGold	bofh@example.com	office	C2:6E:1F:BD:48:94		TP-LINK TECHNOLOGIES CO.,LTD.			2016-06-27 17:33:23

Figura 4.21: Rede de teste no laboratório composta por quatro APs.

Interfaces

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento	Timestamp
3564	1	Dot11Radio0	ieee80211 (71)	ON	192.168.109.161	2016-06-27 17:33:23
3565	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.161	2016-06-27 17:33:23
3566	3	Null0	other (1)	ON	192.168.109.161	2016-06-27 17:33:23
3567	4	BVI1	bridge (209)	ON	192.168.109.161	2016-06-27 17:33:23
3568	1	Wireless 802.11G	other (1)	ON	192.168.109.162	2016-06-27 17:33:23
3569	2	Ethernet	ethernetCsmacd (6)	ON	192.168.109.162	2016-06-27 17:33:23
3570	1	Dot11Radio0	ieee80211 (71)	OFF	192.168.109.164	2016-06-27 17:33:23
3571	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.164	2016-06-27 17:33:23
3572	3	Null0	other (1)	ON	192.168.109.164	2016-06-27 17:33:23
3573	4	BVI1	bridge (209)	ON	192.168.109.164	2016-06-27 17:33:23
3574	5	FastEthernet0.3-802.1Q vLAN subif	l2vlan (135)	ON	192.168.109.164	2016-06-27 17:33:23
3575	6	Dot11Radio0.3-802.1Q vLAN subif	l2vlan (135)	OFF	192.168.109.164	2016-06-27 17:33:23
3576	9	FastEthernet0.5-802.1Q vLAN subif	l2vlan (135)	ON	192.168.109.164	2016-06-27 17:33:23
3577	10	Dot11Radio0.5-802.1Q vLAN subif	l2vlan (135)	OFF	192.168.109.164	2016-06-27 17:33:23

Figura 4.22: Interfaces dos APs da rede de teste no laboratório.

3578	1	lo	softwareLoopback (24)	ON	192.168.109.165	2016-06-27 17:33:23
3579	2	eth0	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24
3580	3	eth1	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24
3581	5	br-lan	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24
3582	7	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 17:33:24
3583	8	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 17:33:24
3584	9	wlan0-1	ethernetCsmacd (6)	OFF	192.168.109.165	2016-06-27 17:33:24
3585	10	wlan0	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24
3586	11	wlan0-1	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24
3587	12	wlan0-2	ethernetCsmacd (6)	ON	192.168.109.165	2016-06-27 17:33:24

Figura 4.23: Interfaces dos APs da rede de teste no laboratório (continuação).

SSID

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC	Timestamp
2056	teste1Cisco1100	ON	00:12:D9:42:95:90	0	OFF	00:12:D9:42:95:90	2016-06-27 17:33:24
2057	teste1Dlink	ON	00:13:46:6F:C5:E3	1	OFF	00:13:46:6F:C5:E3	2016-06-27 17:33:24
2058	teste2Dlink	ON	00:13:46:6F:C5:E3	1	OFF	00:13:46:6F:C5:E3	2016-06-27 17:33:24
2059	teste3Dlink	OFF	00:13:46:6F:C5:E3	4	OFF	00:13:46:6F:C5:E3	2016-06-27 17:33:24
2060	teste1Cisco1200	OFF	00:0E:83:78:4C:C0	3	OFF	00:0E:83:78:4C:C0	2016-06-27 17:33:24
2061	teste2Cisco1200	OFF	00:0E:83:78:4C:C1	5	OFF	00:0E:83:78:4C:C0	2016-06-27 17:33:24
2062		ON	C4:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 17:33:24
2063		ON	C6:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 17:33:24
2064		ON	C2:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94	2016-06-27 17:33:24

Figura 4.24: SSIDs dos APs da rede de teste no laboratório.

Estações

ID	Nome	Endereço IP	Endereço MAC	SSID	Modo	Tipo	Endereço IP do equipamento	Endereço MAC	Timestamp
1137	00	192.168.109.122	78:7E:61:A4:FE:D3	teste1Cisco1100	ieee802dot11g	unknown	192.168.109.161	00:12:D9:42:95:90	2016-06-27 17:33:24
1138			00:22:F4:21:7D:29	teste2Dlink	802.11g		192.168.109.162	00:13:46:6F:C5:E3	2016-06-27 17:33:25
1139			70:18:8B:F4:5E:E5	teste1Dlink	802.11g		192.168.109.162	00:13:46:6F:C5:E3	2016-06-27 17:33:25

Figura 4.25: Estações conectadas aos APs da rede de teste no laboratório.

4.3.3 Cenário de teste - rede do INESC TEC

Foi utilizada uma segunda rede, mais complexa, pertencente ao INESC TEC. Também esta é composta por quatro APs, apesar de três deles serem *dual radio*. Apresentam-se, de seguida, as informações obtidas através da ferramenta desenvolvida.

Rede

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão	Timestamp
1217	192.168.129.32	ap1ad.inescn.pt	Joao Neves	INESCP,piso1AD	0C:D9:96:76:DF:20	1	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33
1218	192.168.129.32	ap1ad.inescn.pt	Joao Neves	INESCP,piso1AD	0C:D9:96:7A:60:20	36	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33
1219	192.168.129.34	ap2ae.inescn.pt	Joao Neves	INESCP,piso2AE	0C:D9:96:9D:6B:10	11	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33
1220	192.168.129.34	ap2ae.inescn.pt	Joao Neves	INESCP,piso2AE	0C:D9:96:87:5E:20	36	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33
1221	192.168.129.37	ap3be.inescn.pt	Joao Neves	INESCP,piso3BE	00:24:C4:8E:66:C0	6	Cisco Systems	AIR-AP1131G	6M30.29	2016-07-04 14:52:33
1222	192.168.129.41	ap1ac.inescn.pt	Joao Neves	INESCP,piso1AC	0C:D9:96:9D:67:10	1	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33
1223	192.168.129.41	ap1ac.inescn.pt	Joao Neves	INESCP,piso1AC	0C:D9:96:87:5A:20	36	Cisco Systems	AIR-AP1140G		2016-07-04 14:52:33

Figura 4.26: Rede do INESC TEC.

Interfaces

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento	Timestamp
5798	1	Dot11Radio0	ieee80211 (71)	ON	192.168.129.32	2016-07-04 14:52:33
5799	2	Dot11Radio1	ieee80211 (71)	ON	192.168.129.32	2016-07-04 14:52:33
5800	3	GigabitEthernet0	ethernetCsmacd (6)	ON	192.168.129.32	2016-07-04 14:52:33
5801	4	Null0	other (1)	ON	192.168.129.32	2016-07-04 14:52:33
5802	5	Dot11Radio0.2	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5803	6	Dot11Radio0.5	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5804	7	Dot11Radio0.11	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5805	8	Dot11Radio0.21	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5806	9	Dot11Radio1.2	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5807	10	Dot11Radio1.5	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5808	11	Dot11Radio1.11	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5809	12	Dot11Radio1.21	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5810	13	GigabitEthernet0.2	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5811	14	GigabitEthernet0.5	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5812	15	GigabitEthernet0.11	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5813	16	GigabitEthernet0.21	l2vlan (135)	ON	192.168.129.32	2016-07-04 14:52:33
5814	17	BVI1	bridge (209)	ON	192.168.129.32	2016-07-04 14:52:33
5815	1	Dot11Radio0	ieee80211 (71)	ON	192.168.129.34	2016-07-04 14:52:33
5816	2	Dot11Radio1	ieee80211 (71)	ON	192.168.129.34	2016-07-04 14:52:33
5817	3	GigabitEthernet0	ethernetCsmacd (6)	ON	192.168.129.34	2016-07-04 14:52:33
5818	4	Null0	other (1)	ON	192.168.129.34	2016-07-04 14:52:33

Figura 4.27: Interfaces dos APs da rede do INESC TEC.

5819	5	Dot11Radio0.2	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5820	6	Dot11Radio0.5	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5821	7	Dot11Radio0.11	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5822	8	Dot11Radio0.21	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5823	9	Dot11Radio1.2	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5824	10	Dot11Radio1.5	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5825	11	Dot11Radio1.11	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5826	12	Dot11Radio1.21	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5827	13	GigabitEthernet0.2	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5828	14	GigabitEthernet0.5	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5829	15	GigabitEthernet0.11	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5830	16	GigabitEthernet0.21	l2vlan (135)	ON	192.168.129.34	2016-07-04 14:52:33
5831	17	BVI1	bridge (209)	ON	192.168.129.34	2016-07-04 14:52:33
5832	1	Dot11Radio0	ieee80211 (71)	ON	192.168.129.37	2016-07-04 14:52:33
5833	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.129.37	2016-07-04 14:52:33
5834	3	Null0	other (1)	ON	192.168.129.37	2016-07-04 14:52:33
5835	4	Dot11Radio0.2	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5836	5	Dot11Radio0.5	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5837	6	Dot11Radio0.11	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5838	7	Dot11Radio0.21	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5839	8	FastEthernet0.2	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5840	9	FastEthernet0.5	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5841	10	FastEthernet0.11	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5842	11	FastEthernet0.21	l2vlan (135)	ON	192.168.129.37	2016-07-04 14:52:33
5843	12	BVI1	bridge (209)	ON	192.168.129.37	2016-07-04 14:52:33

Figura 4.28: Interfaces dos APs da rede do INESC TEC (continuação).

5844	13	Virtual-Dot11Radio0	ieee80211 (71)	OFF	192.168.129.37	2016-07-04 14:52:33
5845	14	Virtual-Dot11Radio0.2	l2vlan (135)	OFF	192.168.129.37	2016-07-04 14:52:33
5846	15	Virtual-Dot11Radio0.5	l2vlan (135)	OFF	192.168.129.37	2016-07-04 14:52:33
5847	16	Virtual-Dot11Radio0.11	l2vlan (135)	OFF	192.168.129.37	2016-07-04 14:52:33
5848	17	Virtual-Dot11Radio0.21	l2vlan (135)	OFF	192.168.129.37	2016-07-04 14:52:33
5849	1	Dot11Radio0	ieee80211 (71)	ON	192.168.129.41	2016-07-04 14:52:33
5850	2	Dot11Radio1	ieee80211 (71)	ON	192.168.129.41	2016-07-04 14:52:33
5851	3	GigabitEthernet0	ethernetCsmacd (6)	ON	192.168.129.41	2016-07-04 14:52:33
5852	4	Null0	other (1)	ON	192.168.129.41	2016-07-04 14:52:33
5853	5	Dot11Radio0.2	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5854	6	Dot11Radio0.5	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5855	7	Dot11Radio0.11	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5856	8	Dot11Radio0.21	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5857	9	Dot11Radio1.2	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5858	10	Dot11Radio1.5	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5859	11	Dot11Radio1.11	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5860	12	Dot11Radio1.21	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5861	13	GigabitEthernet0.2	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5862	14	GigabitEthernet0.5	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5863	15	GigabitEthernet0.11	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5864	16	GigabitEthernet0.21	l2vlan (135)	ON	192.168.129.41	2016-07-04 14:52:33
5865	17	BVI1	bridge (209)	ON	192.168.129.41	2016-07-04 14:52:33

Figura 4.29: Interfaces dos APs da rede do INESC TEC (continuação).

SSID

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC	Timestamp
2757	INESCP-servicos	OFF	0C:D9:96:76:DF:20	2	OFF	0C:D9:96:76:DF:20	2016-07-04 14:52:33
2758	eduroam	ON	0C:D9:96:76:DF:21	11	OFF	0C:D9:96:76:DF:20	2016-07-04 14:52:33
2759	inescp-guest	ON	0C:D9:96:76:DF:22	21	OFF	0C:D9:96:76:DF:20	2016-07-04 14:52:33
2760	inescporto	ON	0C:D9:96:76:DF:23	5	OFF	0C:D9:96:76:DF:20	2016-07-04 14:52:33
2761	INESCP-servicos	OFF	0C:D9:96:7A:60:20	2	OFF	0C:D9:96:7A:60:20	2016-07-04 14:52:33
2762	eduroam	ON	0C:D9:96:7A:60:21	11	OFF	0C:D9:96:7A:60:20	2016-07-04 14:52:33
2763	inescp-guest	ON	0C:D9:96:7A:60:22	21	OFF	0C:D9:96:7A:60:20	2016-07-04 14:52:33
2764	inescporto	ON	0C:D9:96:7A:60:23	5	OFF	0C:D9:96:7A:60:20	2016-07-04 14:52:33
2765	INESCP-servicos	OFF	0C:D9:96:9D:6B:10	2	OFF	0C:D9:96:9D:6B:10	2016-07-04 14:52:33
2766	eduroam	ON	0C:D9:96:9D:6B:11	11	OFF	0C:D9:96:9D:6B:10	2016-07-04 14:52:33
2767	inescp-guest	ON	0C:D9:96:9D:6B:12	21	OFF	0C:D9:96:9D:6B:10	2016-07-04 14:52:33
2768	inescporto	ON	0C:D9:96:9D:6B:13	5	OFF	0C:D9:96:9D:6B:10	2016-07-04 14:52:33
2769	INESCP-servicos	OFF	0C:D9:96:87:5E:20	2	OFF	0C:D9:96:87:5E:20	2016-07-04 14:52:33
2770	eduroam	ON	0C:D9:96:87:5E:21	11	OFF	0C:D9:96:87:5E:20	2016-07-04 14:52:33
2771	inescp-guest	ON	0C:D9:96:87:5E:22	21	OFF	0C:D9:96:87:5E:20	2016-07-04 14:52:33
2772	inescporto	ON	0C:D9:96:87:5E:23	5	OFF	0C:D9:96:87:5E:20	2016-07-04 14:52:33
2773	INESCP-servicos	OFF	00:24:C4:8E:66:C0	2	OFF	00:24:C4:8E:66:C0	2016-07-04 14:52:33
2774	eduroam	OFF	00:24:C4:8E:66:C1	11	OFF	00:24:C4:8E:66:C0	2016-07-04 14:52:33
2775	inescp-guest	OFF	00:24:C4:8E:66:C2	21	OFF	00:24:C4:8E:66:C0	2016-07-04 14:52:33
2776	inescporto	OFF	00:24:C4:8E:66:C3	5	OFF	00:24:C4:8E:66:C0	2016-07-04 14:52:33
2777	INESCP-servicos	OFF	0C:D9:96:9D:67:10	2	OFF	0C:D9:96:9D:67:10	2016-07-04 14:52:33

Figura 4.30: SSIDs pertencentes aos APs da rede do INESC TEC.

2778	eduroam	ON	0C:D9:96:9D:67:11	11	OFF	0C:D9:96:9D:67:10	2016-07-04 14:52:33
2779	inescp-guest	ON	0C:D9:96:9D:67:12	21	OFF	0C:D9:96:9D:67:10	2016-07-04 14:52:33
2780	inescporto	ON	0C:D9:96:9D:67:13	5	OFF	0C:D9:96:9D:67:10	2016-07-04 14:52:34
2781	INESCP-servicos	OFF	0C:D9:96:87:5A:20	2	OFF	0C:D9:96:87:5A:20	2016-07-04 14:52:34
2782	eduroam	ON	0C:D9:96:87:5A:21	11	OFF	0C:D9:96:87:5A:20	2016-07-04 14:52:34
2783	inescp-guest	ON	0C:D9:96:87:5A:22	21	OFF	0C:D9:96:87:5A:20	2016-07-04 14:52:34
2784	inescporto	ON	0C:D9:96:87:5A:23	5	OFF	0C:D9:96:87:5A:20	2016-07-04 14:52:34

Figura 4.31: SSIDs pertencentes aos APs da rede do INESC TEC. (continuação)

Estações

ID	Nome	Endereço IP	Endereço MAC	SSID	Modo	Tipo	Endereço IP do equipamento	Endereço MAC	Timestamp
162730		10.40.49.174	08:62:66:42:B8:80	eduroam	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:76:DF:20	2016-07-04 14:52:34
162731	ap1ad	10.40 .25.64		inescporto	ieee802dot11g	pc4500Client	192.168.129.32	0C:D9:96:76:DF:20	2016-07-04 14:52:34
162732		10.40.25.6	34:02:86:91:F5:28	inescporto	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:76:DF:20	2016-07-04 14:52:34
162733		10.40.25.138	78:31:C1:C4:97:D2	inescporto	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:76:DF:20	2016-07-04 14:52:34
162734		10.40.49.159	F0:F6:1C:6A:59:C6	eduroam	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162735		10.40.27.128		inescporto	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162736		10.40.25.202	6C:40:08:9A:8B:DA	inescporto	ieee802dot11g	unknown	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162737	ap1ad	10.40.27.208	88:53:2E:AE:E0:7A	inescporto	ieee802dot11g	pc4500Client	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162738	ap1ad	10.40.25.196	AC:7B:A1:59:01:87	inescporto	ieee802dot11g	pc4500Client	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162739	ap1ad	10.40.25.206	AC:7B:A1:D2:5E:FB	inescporto	ieee802dot11g	pc4500Client	192.168.129.32	0C:D9:96:7A:60:20	2016-07-04 14:52:34
162740		10.40.49.137	34:31:11:E7:4C:65	eduroam	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162741	ap2ae	10.40.27.45		inescporto	ieee802dot11g	pc4500Client	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162742	ap2ae	10.40.25.45	48:51:B7:CA:4D:24	inescporto	ieee802dot11g	pc4500Client	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162743		10.40.27.71	5C:96:9D:7C:18:FF	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162744		10.40.25.245	6C:40:08:B2:74:6A	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162745		10.40.25.111	90:B6:86:B5:1C:87	inescporto	ieee802dot11g	pc4500Client	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162746		10.40.25.118	A8:BB:CF:24:55:56	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162747		10.40.25.2	BC:44:34:19:8F:07	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162748	ap2ae	10.40.27.192	E0:94:67:79:98:2F	inescporto	ieee802dot11g	pc4500Client	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162749		10.40.27.235	F4:5C:89:9D:0F:BD	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34
162750		10.40.31.121	64:80:99:94:11:B4	inescp-guest	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:9D:6B:10	2016-07-04 14:52:34

Figura 4.32: Estações conectadas aos APs da rede do INESC TEC.

162751		10.40.49.148	00:08:22:25:4A:2A	eduroam	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:87:5E:20	2016-07-04 14:52:34
162752		10.40.49.181	A0:ED:CD:69:A9:B3	eduroam	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:87:5E:20	2016-07-04 14:52:34
162753		10.40.25.150	6C:40:08:B6:9B:22	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:87:5E:20	2016-07-04 14:52:34
162754		10.40.27.15	A4:5E:60:C4:F8:09	inescporto	ieee802dot11g	unknown	192.168.129.34	0C:D9:96:87:5E:20	2016-07-04 14:52:34
162755		10.40.49.130	10:2A:B3:16:8C:81	eduroam	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162756		10.40.49.169	28:9A:FA:78:D6:9D	eduroam	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162757	ap3be	10.40.49.155	68:5D:43:18:40:6B	eduroam	ieee802dot11g	pc4500Client	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162758		10.40.27.12	20:68:9D:0E:D3:E2	inescporto	ieee802dot11g	pc4500Client	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162759		10.40.25.230	28:E3:47:E9:AA:21	inescporto	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162760		10.40.27.184	54:27:1E:20:05:6D	inescporto	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162761		10.40.27.138	68:A3:C4:7F:7F:70	inescporto	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162762		10.40.25.81		inescporto	ieee802dot11g	unknown	192.168.129.37	00:24:C4:8E:66:C0	2016-07-04 14:52:34
162763		10.40.49.184	00:04:4B:5A:16:F2	eduroam	ieee802dot11g	unknown	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162764		10.40.27.215	00:23:6C:85:BF:A5	inescporto	ieee802dot11g	unknown	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162765		10.40.27.179	28:C6:71:01:0E:C4	inescporto	ieee802dot11g	unknown	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162766	ap1ac	10.40.25.157	34:02:86:91:F3:8E	inescporto	ieee802dot11g	pc4500Client	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162767	ap1ac	10.40.25.133		inescporto	ieee802dot11g	pc4500Client	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162768		10.40.25.145	BC:72:B1:58:82:A5	inescporto	ieee802dot11g	pc4500Client	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162769		10.40.25.66	F8:CF:C5:D8:22:50	inescporto	ieee802dot11g	unknown	192.168.129.41	0C:D9:96:9D:67:10	2016-07-04 14:52:34
162770		10.40.25.75		inescporto	ieee802dot11g	unknown	192.168.129.41	0C:D9:96:87:5A:20	2016-07-04 14:52:34

Figura 4.33: Estações conectadas aos APs da rede do INESC TEC (continuação).

Capítulo 5

Conclusões

Este trabalho teve como objetivo o desenvolvimento de uma interface *web* para gerir, de uma forma centralizada e utilizando o protocolo de gestão SNMP, uma rede composta por *access points* Wi-Fi autónomos.

Pretendeu-se que esta ferramenta fosse capaz de fazer uma pesquisa automática da rede requerida e que, para um qualquer fabricante, fosse capaz de comunicar com o AP e retirar informações relevantes, como os SSIDs, as VLANs e a localização, apresentando, por fim, os resultados na interface gráfica.

Assim sendo, foi feito um estudo prévio sobre as MIBs de onde se pode concluir que existem duas MIBs normalizadas para a gestão de APs: a MIB-II e a MIB IEEE802dot11, esta última, tal como o nome indica, baseada na norma 802.11 do IEEE. A ideia inicial era utilizar ambas as MIBs em todos os APs para retirar toda a informação essencial e informação acerca dos SSIDs. Numa segunda fase, iria ser necessário utilizar as MIBs privadas de cada fabricante para se obter informações específicas sobre as estações associadas.

Após testes utilizando vários APs de diferentes fabricantes foi possível concluir que tal abordagem não era possível: nem todos os APs têm a MIB IEEE802dot11 implementada. Dentro dos APs que têm essa MIB implementada, nem todos apresentam a versão mais recente, existindo algumas diferenças na implementação, principalmente ao nível dos SSIDs.

Para colmatar estes imprevistos, foram desenvolvidas duas alternativas: a primeira, utilizando a MIB-II e a MIB IEEE802dot11 para retirar o máximo de informação possível sobre o AP, usando as MIBs privadas apenas para as informações relevantes e não contidas nas MIBs normalizadas. A segunda alternativa passa por se desenvolver um módulo completo, obtendo todas as informações, através apenas da MIB-II e da MIB desenvolvida por esse fabricante.

Através deste estudo e dos testes realizados nos APs é possível concluir que as MIBs privadas são implementadas de forma bastante diferente entre si, não seguindo nenhuma norma ou raciocínio comum. Alguns equipamentos têm erros de configuração graves, como é o caso do D-Link, que nos apresenta o endereço da interface rádio e *ethernet* com o mesmo endereço MAC e o parâmetro *IfOperStatus* da MIB-II sempre igual a um, mesmo quando as interfaces são desligadas.

Também no AP TP-Link, sempre que é adicionado um novo SSID, o endereço MAC novo correspondente, em vez de ser igual ao original incrementado no último octeto, é igual ao original sendo o incremento feito no primeiro octeto do endereço. Assim, o OUI do equipamento (os três primeiros endereços que correspondem ao fabricante) é alterado.

A alteração das configurações do AP e dos SSIDs é também possível através desta ferramenta, estando apenas limitada pela permissão dos objetos.

Na interface gráfica é possível observar todas as informações detalhadas do AP, como os seus endereços MAC e IP, o canal de transmissão, as suas interfaces, os SSIDs, as VLANs e as estações conectadas, bem como os seus atributos. É também apresentado um esquema da localização relativa dos APs e das estações conectadas.

Concluindo, através deste trabalho foi disponibilizada uma ferramenta *open-source*, que permite aceder às informações numa qualquer aplicação *web*, podendo ser instalada independentemente do sistema operativo. Este projeto faz com que não seja necessária a utilização de *software* proprietário ou de controladores para a gestão dos APs. O principal factor inovador é o facto de se conseguir identificar automaticamente, numa infraestrutura de rede, os APs e ser possível monitorizá-los e alterar algumas das suas configurações, independentemente do seu fabricante.

5.1 Trabalho Futuro

Como sugestão de trabalho futuro propõe-se a implementação de notificações, através de *traps* SNMP, indicando um histórico do movimento das estações entre APs e SSIDs e identificando situações de conflito, como por exemplo quando uma estação se encontra localizada à mesma distância de dois APs.

Além disso, seria de extrema utilidade, o desenvolvimento de uma aplicação que integrasse este projeto de gestão e monitorização e que permitisse ao administrador da rede identificar e bloquear o acesso de certas estações à rede ou a determinados conteúdos.

Por fim, uma possível implementação deste projeto seria a sua aplicação em *cloud*, estando assim a informação da rede acessível em qualquer dispositivo e em qualquer lugar.

Anexo A

Verificação da Solução

A.1 AP Cisco 1200

Hostname Cisco1200

Home: Summary Status		
Association		
Clients: 0		Repeaters: 0
Network Identity		
IP Address		192.168.109.164
MAC Address		000e.83bc.c4b0
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	000e.83bc.c4b0	100Mb/s
Radio0-802.11G	000e.8378.4cc0	54.0Mb/s

(a) Informação geral.

Network Interfaces: Radio0-802.11G Status	
Configuration	
Software Status	Disabled
Operational Rates	1.0 , 2.0 , 5.5 , 6.0 , 9.0 , 11.0 , 12.0 , 18.0 , 24.0 , 36.0 , 48.0 , 54.0 Mb/sec
Aironet Extensions	Enabled
Current Radio Channel	2427 MHz Channel 4
Role in Network	Access Point

(b) Interface Rádio.

Service Set Identifiers (SSIDs)			
SSID	VLAN	Radio	BSSID/Guest Mode
teste1Cisco1200	3	Radio0-802.11G	000e.8378.4cc0 ✓
teste2Cisco1200	5	Radio0-802.11G	000e.8378.4cc1 ✓

(c) SSIDs.

Figura A.1: Informação sobre o AP Cisco 1200 retirada da interface gráfica do equipamento.

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão
1135	192.168.109.164	Cisco1200.Cisco	Isabel Fragoso	Netlab	00:0E:83:78:4C:C0	4	Cisco Systems	AIR-MP21G	6M11.05

(a) Informação geral.

Interfaces

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento
3594	1	Dot11Radio0	ieee80211 (71)	OFF	192.168.109.164
3595	2	FastEthernet0	ethernetCsmacd (6)	ON	192.168.109.164
3596	3	Null0	other (1)	ON	192.168.109.164
3597	4	BVI1	bridge (209)	ON	192.168.109.164
3598	5	FastEthernet0.3-802.1Q vLAN subif	l2vlan (135)	ON	192.168.109.164
3599	6	Dot11Radio0.3-802.1Q vLAN subif	l2vlan (135)	OFF	192.168.109.164
3600	9	FastEthernet0.5-802.1Q vLAN subif	l2vlan (135)	ON	192.168.109.164
3601	10	Dot11Radio0.5-802.1Q vLAN subif	l2vlan (135)	OFF	192.168.109.164

(b) Interfaces.

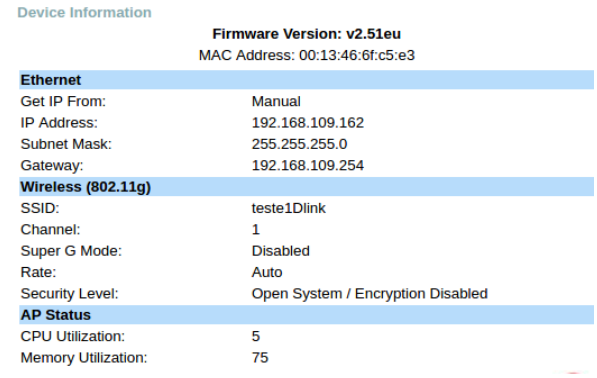
SSID

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC
2069	teste1Cisco1200	OFF	00:0E:83:78:4C:C0	3	OFF	00:0E:83:78:4C:C0
2070	teste2Cisco1200	OFF	00:0E:83:78:4C:C1	5	OFF	00:0E:83:78:4C:C0

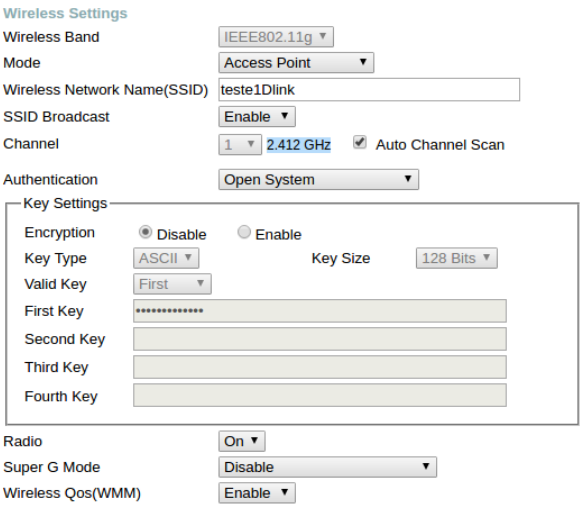
(c) SSIDs.

Figura A.2: Informação sobre o AP Cisco 1100 retirada da ferramenta desenvolvida.

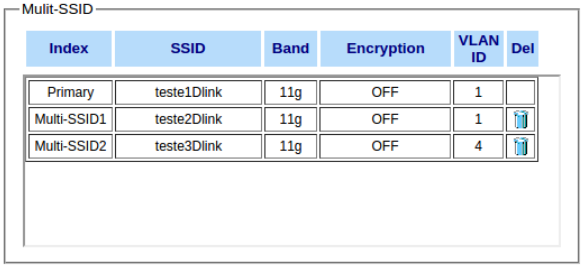
A.2 AP D-Link



(a) Informação geral.



(b) Interface Rádio e SSID principal.



(c) SSIDs.

Figura A.3: Informação sobre o AP D-Link retirada da interface gráfica do equipamento.

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão
1134	192.168.109.162	Dlink2100	Isabel Fragoso	Netlab	00:13:46:6F:C5:E3	1	D-Link Corporation		v2.51eu

(a) Informação geral.

Interfaces

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento
3592	1	Wireless 802.11G	other (1)	ON	192.168.109.162
3593	2	Ethernet	ethernetCsmacd (6)	ON	192.168.109.162

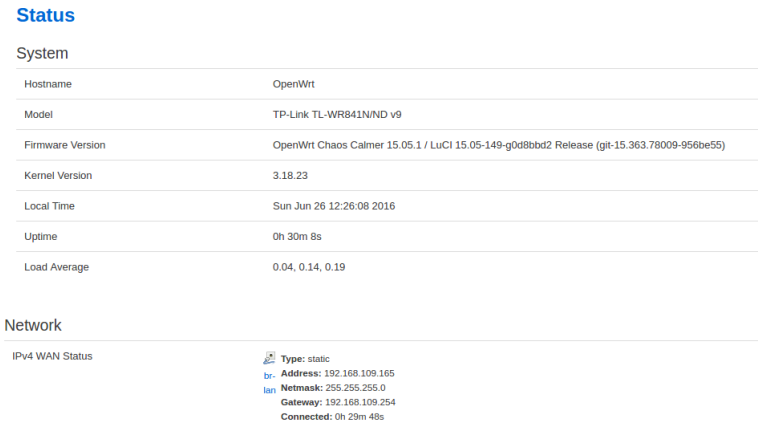
(b) Interfaces.

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC
2066	teste1Dlink	ON	00:13:46:6F:C5:E3	1	OFF	00:13:46:6F:C5:E3
2067	teste2Dlink	ON	00:13:46:6F:C5:E3	1	OFF	00:13:46:6F:C5:E3
2068	teste3Dlink	OFF	00:13:46:6F:C5:E3	4	OFF	00:13:46:6F:C5:E3

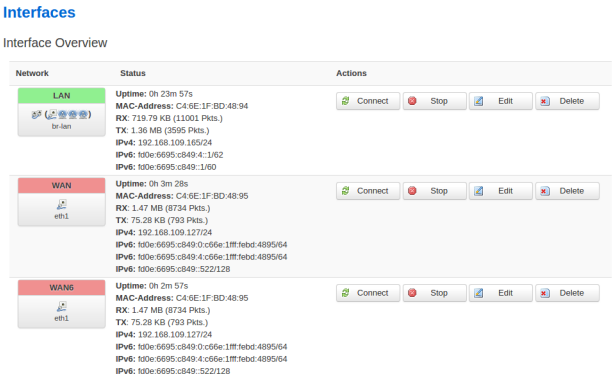
(c) SSIDs.

Figura A.4: Informação sobre o AP D-Link retirada da ferramenta desenvolvida.

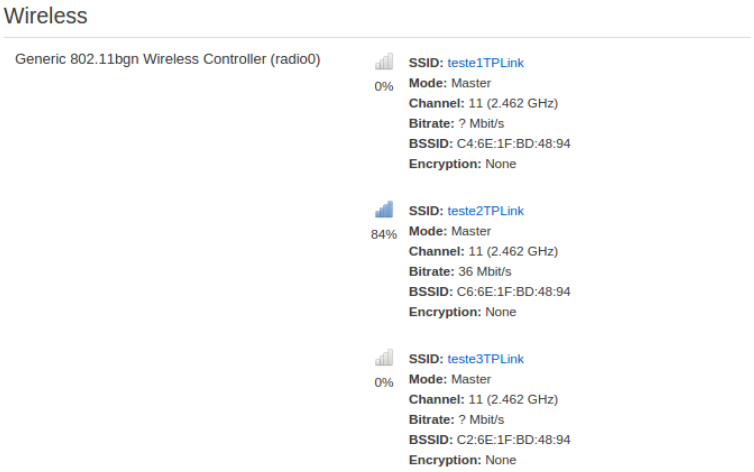
A.3 AP TP-Link



(a) Informação geral.



(b) Interfaces.



(c) SSIDs.

Figura A.5: Informação sobre o AP TP-Link retirada da interface gráfica do equipamento.

ID	Endereço IP	Nome	Contacto	Localização	Endereço MAC da interface rádio	Canal	Fabricante	Modelo	Versão
1136	192.168.109.165	HeartOfGold	bofh@example.com	office	C2:6E:1F:BD:48:94		TP-LINK TECHNOLOGIES CO.,LTD.		

(a) Informação geral.

ID	Índice	Descrição	Tipo	Estado	Endereço IP do equipamento
3602	1	lo	softwareLoopback (24)	ON	192.168.109.165
3603	2	eth0	ethernetCsmacd (6)	ON	192.168.109.165
3604	3	eth1	ethernetCsmacd (6)	ON	192.168.109.165
3605	5	br-lan	ethernetCsmacd (6)	ON	192.168.109.165
3606	7	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165
3607	8	wlan0	ethernetCsmacd (6)	OFF	192.168.109.165
3608	9	wlan0-1	ethernetCsmacd (6)	OFF	192.168.109.165
3609	10	wlan0	ethernetCsmacd (6)	ON	192.168.109.165
3610	11	wlan0-1	ethernetCsmacd (6)	ON	192.168.109.165
3611	12	wlan0-2	ethernetCsmacd (6)	ON	192.168.109.165

(b) Interfaces.

ID	SSID	Broadcast	BSSID	VLAN	Autenticação	Endereço MAC
2071		ON	C4:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94
2072		ON	C6:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94
2073		ON	C2:6E:1F:BD:48:94	0	OFF	C4:6E:1F:BD:48:94

(c) SSIDs.

Figura A.6: Informação sobre o AP TP-Link retirada da ferramenta desenvolvida.

Bibliografia

[1] IEEE, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Standards Association*, 2012.

[2] E. S. L. Yang, P. Zerfos, "Arquitecture taxonomy for control and provisioning of wireless access points (CAPWAP)," *RFC 4118*, 2005.

[3] V. K. Garg, *Wireless Communications and Networking*. Elsevier Inc., 2007.

[4] V. L. Yu-Kwong Kwok, *Wireless Internet and Mobile Computing*. John Wiley & Sons, Inc., 2007.

[5] S. Rackley, *Wireless Networking Technology - From Principles to Successful Implementation*. Newnes, 2007.

[6] K. R. James Kurose, *Computer Networking - A Top-Down Approach*. Pearson Education, Inc, 5th ed., 2010.

[7] C. F. A. Mendonça, "Gestão de uma infra-estrutura de rede wi-fi com recurso ao snmp," Master's thesis, Faculdade de Engenharia da Universidade do Porto, 7 2008.

[8] K. J. S. Douglas R. Mauro, *Essential SNMP*. O'Reilly Media, Inc., 2005.

[9] R. P. S. de Castro Lopes, *Gestão Distribuída em SNMP*. PhD thesis, Universidade de Aveiro, 2002.

[10] M. J. J.Case, M.Fedor, "A simple network management protocol (snmp)," *RFC 1157*, 1990.

[11] J. Neves, "Apontamentos da disciplina de planeamento e gestão de redes," 2014.

[12] K. M. R. Presuhn, J. Case, "Version 2 of the protocol operations for the simple network management protocol (snmp)," *RFC 3416*, 2002.

[13] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Addison Wesley Longman, Inc., 1999.

[14] S. Harnedy, *Total SNMP: Exploring the Simple Network Management Protocol*. Prentice-Hall PTR, 1998.

[15] "Hp imc wireless services manager software." http://h17007.www1.hp.com/us/en/networking/products/network-management/IMC_WSM_Software/. (Disponível em 18/01/2016).

[16] "Cisco prime infrastructure." http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html. (Disponível em 18/01/2016).

[17] "Airwave network management." http://www.arubanetworks.com/products/networking/management/airwave/. (Disponível em 18/01/2016).

[18] "Ruckus unleashed." http://www.ruckuswireless.com/products/system-management-control/unleashed. (Disponível em 18/01/2016).

[19] "Unifi controller software." http://www.ubnt.com/enterprise/software/. (Disponível em 18/01/2016).

[20] "User device tracker." http://www.solarwinds.com/user-device-tracker.aspx. (Disponível em 18/01/2016).

[21] M. R. K. McCloghrie, "Management information base for network management of tcp/ip-based internets: Mib-ii," *RFC 1213*, 1991.

[22] "Manufacturers' oui." http://standards-oui.ieee.org/oui.txt. (Disponível em 15/06/2016).